# COMBINATORIAL DESIGNS AND COVERING CODES

A Thesis Submitted

in Partial Fulfilment of the Requirements

for the Degree of

## DOCTOR OF PHILOSOPHY

*by*

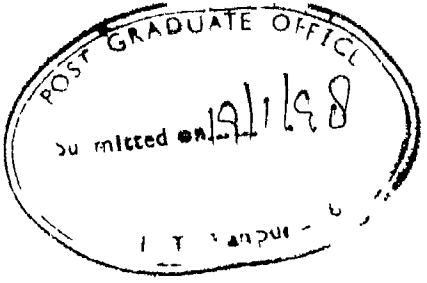
K K P CHANDUKA

*to the*

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

January, 1998




# CERTIFICATE

It is certified that the work contained in the thesis entitled "**Combinatorial Designs and Covering Codes**", by **K K P Chanduka**, has been carried out under my supervision and that this work has not been submitted elsewhere for a degree

**Dr M C Bhandari**
Professor
Department of Mathematics
I I T Kanpur

December, 1997

# ACKNOWLEDGEMENT

I am greatly indebted to my thesis supervisor Prof M C Bhandari for his valuable guidance encouragement and constructive criticism at all stages of this research My discussions with him interspersed throughout the duration of the dissertation were most enlightening His insistence upon clarity of expression has been greatly educational

I am thankful to Prof S P Mohanty for his guidance during the beginning years of this research I express my sincere thanks to Dr A K Lal for his help and stimulating discussions

I must express my special gratitude to Prof Iiro Honkala who promptly responded to my E-mails and provided me with many preprints and reprints which were very much useful for my research work

I take this opportunity to thank all who have helped me in providing moral support during the difficult period of my Ph D programme I owe a lot to my friends who have made my stay at IIT Kanpur a pleasant and memorable one

I am indebted to my parents and family members for their constant encouragement and support I am grateful to Mr Piari Charan Das who has been a source of inspiration throughout

I owe a lot to my wife Bandana who spared me to work for long hours during the final stage of this research work

I am thankful to Mr R N Srivastava for typing this dissertation

K K P Chanduka

# CONTENTS

# NOMENCLATURE

| | |
|---|---|
| $\mathbb{F}_q$ | Finite field if q is a prime power otherwise the set of integers modulo q |
| GF(q) | Galois field with q elements |
| $\mathbb{F}_q^n$ | The set of all n-tuples (words) over $\mathbb{F}_q$ |
| $\mathbf{x}$ | Element of $\mathbb{F}_q^n$ |
| $\mathbf{x}(i)$ | ith coordinate of $\mathbf{x}$ |
| $\|S\|$ | Cardinality of the set S |
| $\mathbb{N}$ | Set of natural numbers |
| $\lfloor x \rfloor$ | The *greatest integer* less than or equal to x |
| $\lceil x \rceil$ | The *smallest integer* greater than or equal to x |
| $\binom{n}{r}$ | The combination of n things taken r at a time |
| d(x y) | Hamming distance between the words $\mathbf{x}$ and y |
| d(x S) | Smallest distance of $\mathbf{x}$ from a word in S |
| C | Nonempty subset of $\mathbb{F}_q^n$ called a q-ary code |
| [n k d] | A linear code of length n dimension k and minimum distance d |
| (q n M)R | A q-ary code of length n having M codewords and covering radius R |
| $K_q(n\ R)$ | Minimum cardinality of a q-ary code of length n and covering radius R |
| $t_q[n\ k]$ | The minimal covering radius of a q-ary code of length n and dimension k |
| $\alpha(k\ \lambda\ v)$ | $\equiv \left\lceil \frac{v}{k} \left\lceil \frac{\lambda(v-1)}{k-1} \right\rceil \right\rceil$ i e Schonheim lower bound |
| $\beta(k\ m\ n)$ | $\equiv \left\lceil \frac{mn}{k} \left\lceil \frac{m(n-1)}{k-1} \right\rceil \right\rceil$ |

| | |
|---|---|
| $AD[k\ \lambda\ v]$ | Covering design or ample design of a v-set with block size k such that every 2-subset is contained in at least $\lambda$ blocks |
| $C(k\ \lambda\ v)$ | Minimum number of blocks in an $AD[k\ \lambda\ v]$ |
| $AD^{*}[k\ \lambda\ v]$ | A labelled covering design |
| $GD[k\ m\ \lambda\ v]$ | Group divisible design with k, m $\lambda$ v as the parameters |
| $GD[k\ m\ v]$ | Group divisible design $GD[k\ m\ \lambda\ v]$ with $\lambda = 1$ |
| $GD(k\ m)$ | Set of integers v for which a $GD[k\ m\ v]$ exists |
| $TD[k\ \lambda\ m]$ | Transversal design with k $\lambda$ and m as parameters |
| $TD[k\ m]$ | Transversal design $TD[k\ \lambda\ m]$ with $\lambda = 1$ |
| $TD(k)$ | Set of integers m for which $TD[k\ m]$ exists |
| $GC[k\ m\ n]$ | Group covering design with k m and n as parameters |
| $G(k\ m\ n)$ | Minimum number of blocks in a $GC[k\ m\ n]$ |
| $S_m(n\ 2)$ | Minimum number of rows in any 2-surjective matrix over the alphabets $\mathbb{F}_m$ with n columns |
| ■ | End of the proof |

# SYNOPSIS

Name of the student **K K P Chanduka** Roll No **9010864**

Degree for which submitted **Ph D** Department **Mathematics**

Thesis Title **Combinatorial Designs and Covering Codes**

Name of the Thesis Supervisor **Prof M C Bhandari**

Month and year of thesis submission **December, 1997**

For a positive integer n let $\mathbb{F}_q^n$ be the set of all n-tuples (called *words*) over $\mathbb{F}_q = \{0\ 1\ \ldots\ q-1\}$ A *q-ary code* C of length n is a nonempty subset of $\mathbb{F}_q^n$ If C is in addition a subspace of $\mathbb{F}_q^n$ then C is called a q-ary *linear* code

The *Hamming distance* d(x y) between words $x\ y \in \mathbb{F}_q^n$ is the number of coordinates in which they differ The *sphere* of radius R with center at x is the set $B_R(x) = \{y \in \mathbb{F}_q^n \mid d(x,y) \leq R\}$ The *cardinality* of $B_R(x)$ is denoted by $V_q(n,R)$ i e

$$V_q(n\ R) = \sum_{i=0}^{R} \binom{n}{i} (q-1)^i$$

The *covering radius* of a code is the least positive integer R such that the spheres of radius R around the codewords cover $\mathbb{F}_q^n$ A code $C \subseteq \mathbb{F}_q^n$ is an (q n M)R code if $\bigcup_{c \in C} B_R(c) = \mathbb{F}_q^n$ and $\bigcup_{c \in C} B_{R-1}(c) \neq \mathbb{F}_q^n$ and $|C| = M$ In the dissertation we always assume that C is an (q n M)R code Denote

$$A_t(x) = |\{c \in C \mid d(x\ c) = t\}|$$

For a given n and R let $K_q(n\ R) = \min\{M \mid \text{a } (q\ n\ M)R \text{ code exists}\}$ The problem of determining the value of $K_q(n,R)$ is known as *covering problem* In particular for q = 3 R = 1 this is popularly known as the *'football pool problem'* [81]

Determining $K_q(n\ R)$ is a hard combinatorial problem Only few exact

values for $K_q(n\,R)$ are known Therefore, efforts have been concentrated in finding good lower and upper bound for $K_q(n\,R)$ (see the refererences) The *sphere covering bound* is a trivial lower bound for $K_q(n,R)$ and is given by

$$K_q(n\,R) \geq q^n/V_q(n\,R) \qquad (1)$$

Various analytical methods and counting arguments are used to improve upon the sphere covering bound The most significant improvement is due to van Wee [80] Its basic idea is to estimate the number of words that are covered more than once by Hamming spheres of radius R centered at codewords In [31] Honkala related the class of words that are at a Hamming distance R from the codewords to the covering design problem Later it was generalised by Zhang [88] In [12] Chen and Honkala extended the technique used in [31] to the case $q \geq 3$ and improved the lower bounds for $K_q(n\,R)$ for many values n and R

The aim of the present dissertation is to further improve the existing lower bounds for $K_q(n\,R)$ In the binary case the lower bounds are improved by using simple observation of Zhang's [88] result and Honkala s [31] technique This gives nineteen improvements in [14 Table 6 1] For extending this technique to $q \geq 3$ a new combinatorial design called a *group covering design* has been introduced Many results are obtained in this regard and these are used along with some other lemmas to improve many values of lower bounds for $K_q(n\,R)$ $q \geq 3$

Chapter II of the dissertation gives a brief survey of known results on covering codes and covering designs Besides this few results have been obtained about the covering designs which are a generalisation of some of the results of [21] and [53] Using this, Theorems 1-3 (given below) have been proved giving an improvement to Schonheim lower bound in some general situations Let X be a v-set (set with v elements) and let $\mathcal{B}$ be a collection of k-subsets (called *blocks*) of X Then $(X,\mathcal{B})$ is called a *covering design*

AD[k λ v] if every pair of distinct elements from X is contained in *at least* λ blocks Covering number C(k λ v) is defined by

$$C(k\ \lambda,v) = \min\left\{|\mathcal{B}| \quad (X\ \mathcal{B}) \text{ is an AD}[k\ \lambda\ v]\right\}$$

In [68] Schonheim has shown that $C(k\ \lambda\ v) \geq \left\lceil \frac{v}{k}\left\lceil \frac{\lambda(v-1)}{k-1}\right\rceil\right\rceil \equiv \alpha(k\ \lambda\ v)$ (say) and in [28] Hanani has proved the following theorem

**Theorem 1** Let (X $\mathcal{B}$) be a covering design AD[k λ v] If $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ and $\lambda v(v-1)/(k-1) \equiv -1 \pmod{k}$ then $C(k\ \lambda\ v) \geq \alpha(k\ \lambda\ v) + 1$

We give an alternate proof of the above theorem It is extendable to some other general situations described in the following two theorems

**Theorem 2** Let (X $\mathcal{B}$) be a covering design AD[k λ v], $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ and let $\lambda v(v-1)/(k-1) \equiv -2 \pmod{k}$ If $\lambda(v-k) < (k-1)(k-2)$ then

$$C(k\ \lambda\ v) \geq \alpha(k\ \lambda\ v) + 1$$

**Theorem 3** Let $v \geq k > 3$ be positive integers Let (X $\mathcal{B}$) be a covering design AD[k λ v] $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ and let $\lambda(v)(v-1)/(k-1) \equiv -3 \pmod{k}$ If $2\lambda(v-k) < (k-1)(k-3)$ then $C(k\ \lambda\ v) \geq \alpha(k\ \lambda\ v) + 1$

In Chapter III group divisible designs and group covering designs are discussed Hanani [28] gave the following necessary condition for the existence of a group divisible design

**Theorem 4** If a group divisible design GD[k m 1 mn] exists then
(i) $m(n-1) \equiv 0 \pmod{(k-1)}$ (ii) $nn^2(n-1) \equiv 0 \pmod{k(k-1)}$ (iii) $n \geq k$

For $n > k$ we prove a stronger necessary condition for the existence of a group divisible design GD[k m mn] This is stated in the following theorem

**Theorem 5** If a group divisible design GD[k m mn] exists and $n > k$ then
(i) $m(n-1) \equiv 0 \pmod{k-1}$ (ii) $nm^2(n-1) \equiv 0 \pmod{k(k-1)}$ (iii) $mn \geq k(k-1)+m$

The new condition (iii) proves nonexistence of many group divisible design GD[k m,mn]

In [28], Hanani has shown that if $m \geq k$ then a transversal design TD[k;m] will have two disjoint blocks. It is shown that the converse is also true. Few other general results about the group divisible designs are also established.

Let m, n and k be positive integers with $n \geq k \geq 2$. A triple $(X,\mathcal{G},\mathcal{B})$ where X is a finite set of mn points, $\mathcal{G}$ is a family of nonempty m-subsets (called *groups*) which is a partition of X and $\mathcal{B}$ is a collection of nonempty k-subsets of X (called *blocks*), is a *group covering design* denoted by GC[k,m;n] if

(i) $|G_i \cap B_j| \leq 1$ for every $G_i \in \mathcal{G}$ and every $B_j \in \mathcal{B}$,

(ii) Every pairset $\{x,y\} \subseteq X$ such that x and y belong to distinct groups is contained in *at least* one block of $\mathcal{B}$.

It follows immediately that a covering design AD[k,1;n] is a *group covering design* GC[k,m;n] with m = 1. The *group covering number* denoted by G(k,m;n) is defined as

$$G(k,m;n) = \min\{|\mathcal{B}| : (X,\mathcal{G},\mathcal{B}) \text{ is a group covering design GC[k,m;n]}\}$$

A simple counting argument gives the following lower bound for G(k,m;n).

**Theorem** 6 Let k, n and m be positive integers with $n \geq k \geq 2$. Then

$$G(k,m;n) \geq \left\lceil \frac{mn}{k} \left\lceil \frac{m(n-1)}{k-1} \right\rceil \right\rceil \equiv \beta(k,m;n) \quad \text{(say)}. \qquad (2)$$

In [31], Honkala has also established a similar inequality. Improvement to inequality (2) are found in many situations and are used for improving the lower bounds for q-ary covering codes. Using the results of 2-surjective matrices [69] many exact bounds for the group covering number are obtained.

The following three theorems give improvement to the lower bound for G(k,m;n) given by (2).

**Theorem** 7: Let $(X,\mathcal{G},\mathcal{B})$ be a group covering design GC[k,m;n]. Suppose

that $m(n-1) \equiv 0 \pmod{(k-1)}$ and $nm^2(n-1)/(k-1) \equiv -1 \pmod{k}$ Then $G(k\ m\ n) \geq \beta(k\ m\ n) + 1$

**Theorem 8** Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design $GC[k\ m\ n]$ and let $m(n-1) \equiv 0 \pmod{(k-1)}$ and $nm^2(n-1)/(k-1) \equiv -2 \pmod{k}$ If $m(n-1)/(k-1) < (k+m-2)$ then $G(k\ m\ n) \geq \beta(k\ m\ n) + 1$

**Theorem 9** Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design $GC[k\ m\ n]$ and let $m(n-1) \equiv 0 \pmod{(k-1)}$ and $nm^2(n-1)/(k-1) \equiv -3 \pmod{k}$ If $m(n-1)/(k-1) < \frac{1}{2}(k-1) + m - 1$ then $G(k\ m\ n) \geq \beta(k\ m\ n) + 1$

Let $\Delta(mn+1\ \ m+1) = C(m+1\ \ 1\ \ nm+1) - \alpha(m+1,\ 1\ \ nm+1)$ Using the known bounds on covering number the following theorem further improves the bound given by (2)

**Theorem 10** Let $m \geq n - 1$ Then $G(m+1,m\ \ n) \geq \beta(m+1\ m\ \ n) + \Delta(nm+1\ \ m+1)$

The following two theorems give the exact bounds for $G(k\ m\ n)$ for many class of group covering designs

**Theorem 11** If $n(\geq 2)$ is a positive integer then

$$C(n\ 2\ n) = \min\{M\ \ n \leq \binom{M-1}{t}\ \ M \in \mathbb{N}\} \text{ where } t = \lfloor M/2 \rfloor - 1$$

**Theorem 12** Let $k(\geq 2)$ $n(\geq k)$ and $v$ be positive integers with $(v-1) \equiv 0 \pmod{(k-1)}$ $v(v-1)/(k-1) \equiv -2 \pmod{k}$ $n = (v-1)/(k-1)$ and let $v > k(k-2)+2$ If there exists a minimum covering design $AD[k\ 1\ v]$ with $C(k\ 1\ v) = \alpha(k\ 1\ v)$ then there also exists a minimum group covering design $GC[k\ k-1\ n]$ with $G(k\ k-1\ n) = \lceil n(n-1)(k-1)/k \rceil$

As a special case of Theorem 12 we have the following two corollaries

**Corollary 13** For every positive integer $n \geq 3$ $G(3\ 2\ n) = \lceil 2n(n-1)/3 \rceil$

**Corollary 14** For every positive integer $n \geq 4$ $n \neq 6$

$$G(4,3\ n) = \lceil 3n(n-1)/4 \rceil$$

Let $C$ be a binary covering code of length $n$ and covering radius $R$

The following notations as given in [80] and [31] are needed in Lemma 15 below

$$A = \{x \in \mathbb{F}_2^n \quad d(x\,C) \geq R - 1\} \qquad E_C(V) = \sum_{c\in C} |B_R(c) \cap V| - \Big| \bigcup_{c\in C} B_R(c) \cap V \Big|$$

$$Z_i = \{x \in \mathbb{F}_2^n \quad |B_R(x) \cap C| = i + 1\} \text{ for } i \in \mathbb{N} \qquad Z = \bigcup_{i>0} Z_i$$

For all $j$ $1 \leq j \leq R$

$$Y_j = \Big\{ x \in Z \cap A \quad \text{the largest pairwise distance between the elements in } (B_R(x) \cap C) \text{ is } 2j \text{ or } 2j - 1 \Big\}$$

The following two results are proved in chapter IV

**Lemma 15** For every $x \in Y_j \cap Z_i$ $E_C(B_2(x)) \geq \varepsilon_{ij}$ where

$$\varepsilon_{ij} = (i+1)\left[ 1 + (n-R+1)R + \binom{R}{2} \right] + \binom{R+2}{2} C(R+2 \;\; 1 \;\; n-R-ij+1) - V_2(n\,2)$$

**Theorem 16** Let $n \geq 2R + 1$ Then

$$K(n\,R) \geq \frac{(V_2(n\,2) - \mu + \varepsilon)\, 2^n}{(V_2(n\,2) - \mu)\, V_2(n\,R) + \varepsilon V_2(n\,R-2)}$$

where $\varepsilon = \binom{R+2}{2} C(R+2 \;\; 1 \;\; n-R+1) - \binom{n-R+1}{2}$, $\Delta_j = \binom{R}{2} + j(R-j) + \binom{j}{2}$

$$\mu_1 = 2 + n(R-2) - \binom{R-2}{2} \qquad \mu_2 = \min_{\substack{i \geq 1 \\ 1 \leq j \leq R}} \left\{ \Delta_j + \frac{\varepsilon_{ij} - \varepsilon}{i} \right\}$$

$$\mu = \begin{cases} \mu_2 & \text{if } R = 1 \\ \min\{\mu_1\ \mu_2\} & \text{if } R \geq 2 \end{cases}$$

The above theorem when applied to particular values of n and R gives nineteen improvement in [14 Table 6 1]

In Chapter V of the dissertation we use group covering numbers to give a better estimate of the excess in comparison to [31] The following two results are proved

**Lemma 17** Let $C \leq F_q^n$ be a covering code with covering radius R Then

$$\min_{x \in \mathbb{F}_q^n} \Big\{ A_{R+1}(x) \quad A_0(x) = A_1(x) = \quad = A_{R-2}(x)$$

$$= A_R(x) = A_{R+2}(x) = 0 \;\; A_{R-1}(x) = 1 \Big\} \geq \left\lceil \frac{n - R + 1}{R + 1} \left\lceil \frac{(n-R)(q-1)}{R} \right\rceil \right\rceil$$

**Theorem 18** Let $q \geq 3$ and $n > R$ Then

$$K_q(n\ R) \geq \frac{(V_q(n,2) - \mu + \varepsilon)\ q^n}{(V_q(n\ 2) - \mu)\ V_q(n\ R) + \varepsilon V_q(n\ R-2)}$$

where

$$M_{R-1} = 1 + n(q-1) + (R-1)(n-R/2)(q-1)^2$$

$$M_R = 1 + R(n-R+1)(q-1) + \binom{R}{2} (q-1)^2$$

$$M_{R+1} = \binom{R+2}{2} + R(R+1)(q-2)$$

$$\varepsilon_1 = \binom{R+2}{2} G(R+2,\ q-1,\ n-R+1) - \binom{n-R+1}{2} (q-1)^2$$

$$\varepsilon_2 = \min_{\substack{A_{R+1}(x) \geq 1 \\ A_{R+2}(x) \geq 0}} \left\{ M_{R-1} + A_{R+1}(x)\ M_{R+1} + A_{R+2}(x) \binom{R+2}{2} - V_q(n,2) \right\}$$

$$\varepsilon_3 = \min_{\substack{l \geq l_0 \\ A_{R+2}(x) \geq 0}} \left\{ M_R + (l+1_0)\ M_{R+1} + A_{R+2}(x) \binom{R+2}{2} - V_q(n\ 2) \right\}$$

$$\varepsilon = \min\{\varepsilon_1,\ \varepsilon_2,\ \varepsilon_3\}$$

$$\mu_0 = \binom{R+2}{2} (q-1)^2 + (R-2)(n-R+3)(q-1) + 2$$

$$\mu_1 = 2R^2 - R + 1 - \varepsilon$$

$$\mu = \begin{cases} \mu_1 & \text{if} \quad R = 1 \\ \min\{\mu_0,\ \mu_1\} & \text{if} \quad R \geq 2 \end{cases}$$

# CHAPTER I

# INTRODUCTION

Let $\mathbb{F}_q$ be an alphabet consisting of q elements In order to have an algebraic structure $\mathbb{F}_q$ is usually taken to be a finite field of q elements if q is a prime power otherwise $\mathbb{F}_q$ is the set of integers modulo q In any case the set $\mathbb{F}_q = \{0\ 1\ 2 \quad q-1\}$ is used to denote the elements of the alphabet $\mathbb{F}_q$ For a positive integer n, let $\mathbb{F}_q^n$ be the set of all n-tuples over $\mathbb{F}_q$ (an n-dimensional vector space if q is a prime power) Elements of $\mathbb{F}_q^n$ are called *words* A *covering code* C is a nonempty subset of $\mathbb{F}_q^n$ such that every word in the set $\mathbb{F}_q^n$ is within a specified Hamming distance R the covering radius of at least one codeword (an element of C) Determining $K_q(n\ R)$ the *minimal cardinality* of a covering code of length n and covering radius R is a difficult task in general It is popularly known as the *covering problem* The origin of the covering problem dates back to 1948 when Taussky and Todd [76] considered it in a restricted sense as certain industrial problem In the earliest papers this problem has been studied by many researchers in the group theoretic context [17] [49] [51] [70] [76] [86] and [87] Over the years the problem was reformulated and generalised many times

Actually prior to the publication of the paper [76] by Taussky and Todd the covering problem was a favourite among football pool enthusiasts in European countries In one entry in a football pool one forecasts the outcome of n football matches (*win, lose* or *draw*) To win the first prize all forecasts have to be correct If one wishes to guarantee winning the first prize, irrespective of the outcome of matches, then one has to submit $3^n$ entries To win the second prize one of the forecasts may be incorrect

In order to guarantee the second prize we consider each entry as a word in $\mathbb{F}_3^n$ If the set of entries has covering radius one then winning at least the second prize is guaranteed, no matter what the outcome of the matches is The set of entries is called a *football pool system* and the number of entries is usually denoted by $\sigma(n\ 3)$ or $\sigma_n$ for example see [14], [20] [38] [42], [79] and [83] For further discussion of the early history of the football pool system see [81] In terms of the code parameter

$$\sigma(n\ 3) = K_3(n\ 1)$$

In recent years, covering codes have found applications in Cryptanalysis of Stream Ciphers [39] Minmax Constraint Binary Vector Quantisation (MCBVQ) method (studied for improving subjective quality of compressed binary images) [85] distribution of resources in hypercube computers [48] coding of speech [22] data compression and data transmission [15] A number of other applications of covering code are mentioned in a recent book by Cohen *et al* [14]

In the earliest papers [10], [36]-[38], [49], [51], [67], [71], [73], [76] [86] and [87] only codes with covering radius 1 were treated It is only a development of the early eighties that the covering codes and the covering radius of codes received attention of many researchers, see [14] for an extensive list of papers on these topics Exact values for $K_q(n,R)$ are known only for some special values of the parameters q n and R In the general case, efforts have been concentrated to obtain good lower and upper bounds on $K_q(n,R)$ Good lower bounds are obtained by various analytical methods, whereas for the upper bounds, explicit constructions are given for the covering codes [65]

In early eighties, most improvements *e g*, see [16] and [30] on lower bounds for the minimal cardinality of a covering code are due to the quantity A(n d), the maximal number of codewords in any binary code of

length n and with minimum distance d (cf [50 p 523]) However the most significant improvement on the general lower bound was due to van Wee [80] [82] van Wee introduced the concept of excess and gave an estimation for the number of words that are covered more than once This gave many improvements on the earlier known lower bounds on $K_q(n R)$ Using van Wee's method Honkala [31] and Hou [34] further modified lower bounds on $K_2(n,R)$ Later Chen and Honkala [12] extended this technique to the case $q \geq 3$ and obtained improvements in the lower bounds on $K_q(n R)$ $q \geq 3$ Zhang [88] and Zhang and Lo [89] used *Hamming Association scheme* [50 p 656] to link covering codes to covering designs and obtained linear inequalities satisfied by covering codes These linear inequalities lead to better lower bounds on $K_2(n R)$ In [44] Li and Chen generalised van Wee s and Zhang's methods to obtain further improvements on the lower bounds for $K_2(n R)$ It has recently been discovered that an early paper [35] by Johnson contains e g the main approaches described in [80] and [88] In [23] Habsieger introduced a new technique to further improve the lower bounds for $R = 1$ Recently using some simple observations Bhandari and Durairajan [9] gave many improvements on the lower bounds for $K_q(n R)$

The aim of the present dissertation is to further improve the general lower bounds on $K_q(n R)$ The main techniques and methods used in this dissertation is of combinatorial nature Using some simple observation on Zhang s result [88] we generalise Honkala's technique [31] This generalisation gives nineteen improvements in [14 Table 6 1] for the lower bounds on $K_2(n R)$ For extending this technique to the case $q \geq 3$ we have introduced a new combinatorial design called *group covering design* It can be seen as a generalisation of the well-known covering design (see [57] for extensive references on covering designs) We obtain a few results on group covering designs Using those results many improvements in the existing

lower bounds for $K_q(n, R)$ $q \geq 3$ are obtained

This dissertation is divided into six chapters Chapter II contains preliminary definitions and a brief survey of known results on the covering codes and covering designs Some new results on general improvements of the Schonheim lower bound for covering designs are also presented An updated table from [14] for the covering number is included for the sake of completeness

Chapter III is the most important part of this dissertation The first section in this chapter includes a few new results on group divisible designs A stronger necessary condition for the existence of group divisible design [Theorem 3 1 3] is presented In the second section of this chapter a new combinatorial design called *group covering design* has been introduced Group covering designs apart from being a generalisation of covering designs is also interesting in its own right In chapter V, we have related it to q-ary covering codes and have improved many lower bounds on $K_q(n, R)$ A few results on the group covering designs are established Exact bounds for many class of group covering numbers are given Tight upper and lower bounds for group covering number are also derived in general Finally a table is constructed for group covering numbers for different group size

Chapter IV of this dissertation is devoted to determining better lower bounds for the minimal cardinality of binary covering codes Honkala [31] has related the class of words in $\mathbb{F}_2^n$ that are at a Hamming distance R or R-1 to *exactly* one codeword of a covering code with a given covering radius R, to the covering design problem We use a simple observation of Zhang's result [88] to relate the class of words in $\mathbb{F}_2^n$ that are at a Hamming distance R or R-1 to *one* or *more* codewords, to the covering design problem hence generalising Honkala's method Using the method of estimation of

Honkala [31] we obtain nineteen improvements in the lower bound for $K_2(n, R)$

In Chapter V we relate q-ary covering codes ($q \geq 3$) to group covering designs Using some basic lemmas which have been proved in this chapter and the results of Chapter III we are able to improve the lower bounds for many pair of values of n and R $q \geq 3$ Essentially the results of this chapter are a generalisation of the results of the preceding chapter

The thesis concludes with some general remarks in the last chapter

# CHAPTER II

## PRELIMINARIES AND SURVEY

A nonempty set $\mathbb{F}$ with two binary operations $+$ and $'$, is a *Field* if (i) $(\mathbb{F}, +)$ is an abelian group (ii) $(\mathbb{F}\setminus\{0\}, )$ is an abelian group (iii) distributive laws hold If in addition $\mathbb{F}$ is a finite set $\mathbb{F}$ is called a *finite field* A finite field with q elements exists if and only if q is a prime power A finite field with q elements is unique upto isomorphism and is called the *Galois field* denoted by GF(q) Let $\mathbb{F}_q$ be an alphabet consisting of q elements If q is a prime power $\mathbb{F}_q$ is taken as the Galois field GF(q) otherwise $\mathbb{F}_q$ is the set of integers modulo q For the sake of convenience $\mathbb{F}_q = \{0, 1, 2, \ldots, q-1\}$ is used to denote the elements of the alphabet $\mathbb{F}_q$ Any element $\mathbf{x} = (x_1, \ldots, x_n)$ of $\mathbb{F}_q^n$ the set of all n-tuples over $\mathbb{F}_q$ is called a *word* The *Hamming distance* $d(\mathbf{x}, \mathbf{y})$ between two words $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ is the number of coordinates in which they differ i e

$$d(\mathbf{x}, \mathbf{y}) = |\{i : x(i) \neq y(i)\}|$$

A *q-ary code* C of *length* n is a nonempty subset of $\mathbb{F}_q^n$ C is called a *binary* code if q = 2 and a *ternary* code if q = 3 Moreover if C is a subspace of $\mathbb{F}_q^n$ then C is called a *linear* code The elements of C are called *codewords* The *minimum distance* d of a code C is the smallest of the Hamming distance between any pair of distinct codewords If C is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum distance d then C is called an [n, k, d] code (or simply an [n, k] code if the minimum distance of the code is not specified) If C is *not linear* and $|C| = M$ C is called an (n, M, d) code

Let $\mathbf{x} \in \mathbb{F}_q^n$ A *sphere of radius R with center at* $\mathbf{x}$ is the set

$$B_R(\mathbf{x}) = \{\mathbf{y} \in \mathbb{F}_q^n \quad d(\mathbf{x},\mathbf{y}) \leq R\} \tag{2.1}$$

while a *ring of radius R with center at* $\mathbf{x}$ is the set

$$S_R(\mathbf{x}) = \{\mathbf{y} \in \mathbb{F}_q^n \quad d(\mathbf{x},\mathbf{y}) = R\} \tag{2.2}$$

If R = 1, such a sphere is often called a *rook-domain* [10], [67] It is easy to see that

$$V_q(n\ R) = |B_R(\mathbf{x})| = \sum_{k=0}^{R} \binom{n}{k} (q-1)^k \tag{2.3}$$

The index q is usually omitted in the binary case For other basic definitions the reader is referred to [14] and [50]

## 2.1 Covering Codes

A q-ary code C is called an *R-covering* of $\mathbb{F}_q^n$ ( *i.e. a covering code*) if every word in $\mathbb{F}_q^n$ is within the Hamming distance R from some codeword in C In other words

$$\mathbb{F}_q^n = \bigcup_{\mathbf{c}\in C} B_R(\mathbf{c}) \ ( \equiv B_R(C) \ ) \tag{2.4}$$

The *minimal* value of R for which (2.4) holds is called the *covering radius* of C A q-ary covering code of length n, cardinality M and covering radius R is called a (q,n,M)R code (a (n,M)R code if q = 2) The notation, $t_q[n,k]$ is used for the minimal covering radius of an [n,k] code Usually q, n, k, d and R are called the *parameters* of a code Another important parameter of a code is $K_q(n\ R)$ the *minimal cardinality* of a covering code of length n and covering radius R In other words, it is defined by

$$K_q(n\ R) = \min\{M \quad \text{a } (q,n,M)R \text{ code exists}\} \tag{2.5}$$

The index q is usually dropped in the binary case Determination of $K_3(n\ 1)$ is usually referred to as the *football pool problem* (See [14],[20],[38] [42],[79],[83]) A (q,n,M)R code with $M = K_q(n,R)$ is called an *optimal* code

An obvious lower bound on $K_q(n,R)$ is given by

$$K_q(n,R) \geq q^n / V_q(n,R) \tag{2.6}$$

It is known as the *sphere covering bound* It is obtained by counting the number of elements on both side of (2.4) For given q, n and R, the equality in (2.6) holds if and only if the code is *perfect* i.e. spheres $B_R(c)$ on the right hand side of (2.4) are disjoint In the early seventies van Lint [45] and Tietävainen [77] showed that if q is a prime power, then the only nontrivial perfect codes are codes with the same parameters as the *Hamming* and the *Golay* codes (see [46] for a survey on these results) In case q is not a prime power, the only known perfect codes are the trivial perfect codes (those with R = 0 or R = n) [7], [8], [41] and [66] Besides perfect codes, the codes for which the exact values of $K_q(n,1)$ were known in early seventies are the following $K_q(3,1) = \lceil (q^2 + 1)/2 \rceil$ [36], $K_{pq}(q + 1,1) = p^q q^{q-1}$, if q is a prime power [10], [37], [67], $K_2(4,1) = 4$ and $K_2(5,1) = 7$ [76] $K_2(6,1) = 12$ [72], $K_2(8,1) = 32$ [73], $K_3(5,1) = 27$ [38] and $K_4(4,1) = 24$ [71] The only result added to this list in the last two decades is due to Johnson [35] (later rediscovered by van Wee [80]) and is given by

$$K_2(2^k - 1) = 2^{2^k - k} \qquad k = 1,2, \tag{2.7}$$

This clearly indicates the complexity of calculating the exact values of $K_q(n,R)$ In eighties, many researchers [15], [16] and [22] obtained bounds on the covering radius of binary code which is closely related to determining K(n,R) However, this hardly improves the sphere covering bound on K(n R) In [80] van Wee introduced the concept of *excess* and obtained improvements of the sphere covering bound for many pair of values of n and R Following the notations of [80], the excess $E_C(V)$ on $V(\subseteq \mathbb{F}_q^n)$ by a code $C \subseteq \mathbb{F}_q^n$ with covering radius R is given by

$$E_C(V) = \sum_{c \in C} |B_R(c) \cap V| - \Big| \bigcup_{c \in C} B_R(c) \cap V \Big| \tag{2.8}$$

For each $i = 0\ 1\ 2$ let

$$Z_i(C) = \{x \in \mathbb{F}_q^n \quad |B_R(x) \cap C| = i + 1\} \tag{2.9}$$

and

$$Z(C) = \bigcup_{i>0} Z_i(C) = \{x \in \mathbb{F}_q^n \quad |B_R(x) \cap C| > 1\} \tag{2.10}$$

We denote $Z(C)$ and $Z_i(C)$ by $Z$ and $Z_i$ respectively Then Van Wee [80 Lemmas 1 and 4] has shown that

$$E_C(\mathbb{F}_q^n) = |C| V_q(n\ R) - q^n \tag{2.11}$$

$$E_C(V) = \sum_i i|Z_i \cap V| \tag{2.12}$$

and

$$|C| V_q(n\ R) - q^n = \sum_i i|Z_i| \tag{2.13}$$

By estimating the number of words in $\mathbb{F}_q^n$ that are covered more than once by the spheres of radius R around codewords van Wee has proved the following two theorems

**Theorem 2.1.1** [80 Theorem 9] For all $n\ R \in \mathbb{N}$ with $n > R$ we have

$$K(n\ R) \geq \frac{(n - R + \varepsilon')2^n}{(n - R)V(n\ R) + \varepsilon\ V(n\ R-1)} \tag{2.14}$$

where

$$\varepsilon' = (R + 1)\left\lceil \frac{n + 1}{R + 1} \right\rceil - (n + 1) \tag{2.15}$$

**Theorem 2.1.2** [80, Theorem 10] For all $n\ R \in \mathbb{N}$ with $n \geq 2R$ we have

$$K(n,R) \geq \frac{(V(n\ 2) - \mu + \varepsilon_0)2^n}{(V(n\ 2) - \mu)V(n\ R) + \varepsilon_0 V(n\ R-2)} \tag{2.16}$$

where

$$\mu = (R-1)(R+2)/2, \tag{2.17}$$

$$\varepsilon_0 = \binom{R+2}{2}\left\lceil \frac{\binom{n-R+1}{2}}{\binom{R+2}{2}} \right\rceil - \binom{n-R+1}{2} \qquad (2\,18)$$

In [31] Honkala has modified the van Wee's bound He has shown that the estimation of the excess on spheres of radius 2 centered at the points which have distance R-1 or R to the code C and are covered by **exactly** one codeword is related to the pair covering problem and has proved the following two results

**Lemma** 2 1 3 [31 Lemma 6] Suppose that C is an (n M)R code $n \geq 2R + 1$ and $x \in A \backslash Z$ where $A = \{x \in \mathbb{F}_2^n \quad d(x\,C) \geq R-1\}$ and Z is as in (2 10) with $q = 2$ Then

$$|B_{R+2}(x) \cap C| \geq 1 + C(R+2\,1\,n-R+1) \qquad (2\,19)$$

and

$$E_C(B_2(x)) \geq \varepsilon_0 + (C(R+2\,1\,n-R+1) - m_0)\binom{R+2}{2} \qquad (2\,20)$$

where

$$m_0 = \left\lceil \frac{\binom{n-R+1}{2}}{\binom{R+2}{2}} \right\rceil \qquad \varepsilon_0 = \binom{R+2}{2} m_0 - \binom{n-R+1}{2}$$

**Theorem** 2 1 4 [31 Theorem 2] Assume that $n \geq 2R + 1$ and denote

$$\varepsilon = \varepsilon_0 + (C(R+2\,1\,n-R+1) - m_0)\binom{R+2}{2} \qquad (2\,21)$$

$$\mu_0 = 2 + n(R-2) - \binom{R+2}{2}$$

$$\mu_1 = 2R^2 - R + 1 - \varepsilon$$

where $\varepsilon_0$ and $m_0$ are as in Lemma 2 1 3 Then

$$K(n\,R) \geq \frac{(V(n\,2) - \mu + \varepsilon)2^n}{(V(n\,2) - \mu)V(n,R) + \varepsilon V(n\,R-2)} \qquad (2\,22)$$

where

$$\mu = \begin{cases} \mu_1, & \text{if } R = 1 \\ \min\{\mu_0, \mu_1\}, & \text{if } R \geq 2 \end{cases} \tag{2.23}$$

**Note** In [31] the notation f(v k) is used for the covering number C(k 1 v)

In [12] Chen and Honkala extended this idea to q-ary covering codes and has proved the following two results

**Lemma 2.1.5** [12 Lemma 5] Assume that $\mathbf{x} \in A \backslash Z$ where $A = \{\mathbf{x} \in \mathbb{F}_q^n \quad d(\mathbf{x}, C) \geq R-1\}$ and Z is as in (2.10) Denote

$$M_{R-1} = 1 + n(q-1) + (R-1)(n-R/2)(q-1)^2 \tag{2.24}$$

$$M_R = 1 + R(q-1)(n-R+1) + \binom{R}{2}(q-1)^2 \tag{2.25}$$

$$M_{R+1} = \binom{R+2}{2} + R(R+1)(q-2) \tag{2.26}$$

$$r(x) = \begin{cases} \binom{R+2}{2} \left\lceil -x / \binom{R+2}{2} \right\rceil + x & \text{if } x \leq 0 \\ x & \text{if } x > 0 \end{cases} \tag{2.27}$$

$$l_0 = \lceil (n-R)(q-1)/(R+1) \rceil \quad \text{and} \quad \varepsilon_0 = (R+1)l_0 - (n-R)(q-1)$$

If $d(\mathbf{x}, C) = R - 1$ and $|B_{R+1}(\mathbf{x}) \cap C| = 1$ then

$$E_C(B_2(\mathbf{x})) \geq \varepsilon_1 = \binom{R+2}{2} \left\lceil \frac{(n-R+1)(q-1)}{R+2} \left\lceil \frac{(n-R)(q-1)}{R+1} \right\rceil \right\rceil - \binom{n-R+1}{2}(q-1)^2 \tag{2.28}$$

If $d(\mathbf{x}, C) = R - 1$ and $|B_{R+1}(\mathbf{x}) \cap C| > 1$ then

$$E_C(B_2(\mathbf{x})) \geq \varepsilon_2 = \min_{l>0} \left\{ l(R+1) + r(M_{R-1} + lM_{R+1} - V_q(n,2) - l(R+1)) \right\} \tag{2.29}$$

If $d(\mathbf{x}, C) = R$ then

$$E_C(B_2(\mathbf{x})) \geq \varepsilon_3 = \min_{l>0} \left\{ l(R+1) + \varepsilon_0 + r(M_R + (l+l_0)M_{R+1} - V_q(n,2) - l(R+1) - \varepsilon_0) \right\} \tag{2.30}$$

Therefore for any $x \in A \setminus Z$, we have

$$E_C(B_2(x)) \geq \varepsilon = \min \{\varepsilon_1 \quad \varepsilon_2 \quad \varepsilon_3\} \tag{2.31}$$

**Theorem** 2.1.6 [12 Theorem 4] Assume that $q \geq 3$ and $n > R$ Then

$$K_q(n\ R) \geq \frac{(V_q(n\ 2) - \mu + \varepsilon)q^n}{(V_q(n\ 2) - \mu)V_q(n\ R) + \varepsilon V_q(n\ R-2)} \tag{2.32}$$

where $\varepsilon$ is as in Lemma 2.1.5 and

$$\mu_0 = \binom{R-2}{2}(q-1)^2 + (R-2)(q-1)(n-R+3) + 2$$

$$\mu_1 = 2R^2 - R + 1 - \varepsilon$$

$$\mu = \begin{cases} \mu_1 & \text{if} \quad R = 1 \\ \min\{\mu_0\ \mu_1\} & \text{if} \quad R \geq 2 \end{cases} \tag{2.33}$$

In [88] Zhang has used the quantity $C(k\ 1\ n)$ to derive a linear inequality for binary covering codes In particular he has proved the following result

**Lemma** 2.1.7 [88 Lemma 4] Let C be a binary covering code with length n and covering radius R Let $A_R(x) = |\{c \in C \quad d(x\ c) = R\}|$ Then

$$\min\Big\{A_{R+1}(x) + A_{R+2}(x) \quad A_0(x) = \quad = A_{R-2}(x) = 0 \quad A_{R-1}(x) + A_R(x) = k\Big\} \geq C(R+2\ 1\ n-kR+1) \tag{2.34}$$

In other words for $x \in A \cap Z_{k-1}$ where A and $Z_k$ are as in Lemma 2.1.3 and (2.9) with $(q = 2)$ respectively

$$|B_{R+2}(x) \cap C| \geq k + C(R+2\ 1\ n-kR+1)$$

**Note** In [88] the notation $C(n,k\ 2)$ is used for the covering number $C(k,1\ n)$

A simple observation of the above result (2.34) gives a better estimation of the excess than in [31] for the points which have distance R-1

or R to the code C and are covered by **more than one** codeword This is used to modify the lower bound on K(n,R) further It will be discussed in detail in Chapter IV of the present dissertation

## 2 2 Covering Designs

Let X be a finite set of points and let $\mathcal{B} = \{B_i \mid i \in I\}$ be a collection of subsets (not necessarily distinct) of X called *blocks* The pair $(X,\mathcal{B})$ is called a *design*

Let $v \geq k \geq 2$ and $\lambda$ be positive integers A design $(X\ \mathcal{B})$ is called a *balanced incomplete block design* (BIBD) denoted by $B[k\ \lambda\ v]$ if

(i) $|X| = v$

(ii) Every block has size k

(iii) Every pairset $\{x\ y\} \subseteq X$ is contained in *exactly* $\lambda$ blocks of $\mathcal{B}$

Using a simple counting argument Hanani [28] proved the following necessary conditions for the existence of a BIBD

**Theorem** 2 2 1 [28] If a BIBD $B[k\ \lambda\ v]$ exists then

$$\begin{aligned} &\text{(i)} \quad \lambda(v-1) \equiv 0 \pmod{(k-1)} \\ &\text{(ii)} \quad \lambda v(v-1) \equiv 0 \pmod{k(k-1)} \end{aligned} \tag{2 35}$$

For $3 \leq k \leq 5$ and $v \geq k$ , Hanani [26] [27] has proved that condition (2 35) is sufficient with the exception $v = 15$ $k = 5$ and $\lambda = 2$ On the other hand there are many known cases in which condition (2 35) is not sufficient For example the following inequality of Fisher gives a general result on the nonexistence of BIBD's with parameters v k and $\lambda$ satisfying the condition (2 35)

**Theorem** 2 2 2 [Fisher's inequality] Let $v > k$ and let $B[k\ \lambda\ v]$ be a BIBD Then

$$\frac{\lambda v(v-1)}{k(k-1)} \geq v \tag{2 36}$$

Thus it follows that BIBD's B[6 1 16] B[6 1 21] B[10 3 25] B[12 2 34] etc do not exist Hence efforts have been concentrated to find the parameters $\lambda$ k and v for which BIBD B[k,$\lambda$ v] exist (cf [18] [28] [29] [60] [61] and [90]) In [84] Wilson has proved that condition (2 35) is sufficient for sufficiently large v For further discussion on BIBD see [91]

For given $\lambda$ k and v BIBD's do not always exist To deal with such cases the notion of covering designs were introduced

Let X be a v-set (a set of v elements) and let $\mathcal{B}$ be a collection of k-subsets of X (called *blocks)* The pair (X $\mathcal{B}$) is called a *covering design* or an *ample design* denoted by AD[k $\lambda$ v] if every 2-subset of X is contained in *at least* $\lambda$ blocks of $\mathcal{B}$ A 2-subset is said to be *covered* p times *extra* if it is contained in exactly ($\lambda$ + p) blocks of $\mathcal{B}$ The *replication number* of an element of X is the number of blocks that contains the element

A covering design AD[k $\lambda$ v] with b blocks is said to be *minimum* if for any AD[k $\lambda$ v] with b' blocks one always has $b \leq b'$ The *covering number* C(k $\lambda$ v) is the number of blocks in a minimum covering design AD[k $\lambda$ v] Determining C(k $\lambda$ v) is also known as *pair covering problem* It is easy to see that a covering design AD[k $\lambda$ v] will be a BIBD B[k $\lambda$ v] if and only if $C(k\ \lambda\ v) = \lambda v(v-1)/(k(k-1))$ Hence for positive integers $\lambda$ k and $v(\geq k)$ we have

$$C(k\ \lambda\ v) \geq \frac{\lambda v(v-1)}{k(k-1)}$$

In [68] Schonheim has shown that

$$C(k\ \lambda\ v) \geq \left\lceil \frac{v}{k}\left\lceil\frac{\lambda(v-1)}{k-1}\right\rceil\right\rceil \equiv \alpha(k\ \lambda\ v) \qquad (2\ 37)$$

where $\lceil x \rceil$ is the smallest integer greater than or equal to x $\alpha(k,\lambda\ v)$ is called **Schonheim lower bound** for pair covering problem

The study of covering numbers began with the paper of Fort and Hedlund

[21] They solved the problem of covering of pairs by triples (3-subsets) by showing that (for $\lambda = 1$)

$$C(3\ 1\ v) = \alpha(3\ 1\ v)$$

for all $v \geq 3$ Haggard [24] extended this problem to arbitrary $\lambda$ and proved that

$$C(3\ \lambda\ v) = \begin{cases} \alpha(3\ \lambda\ v)+1 & \text{if both } v \equiv \lambda \equiv 2 \pmod 3 \text{ and } \lambda(v-1) \text{ is even} \\ \alpha(3\ \lambda\ v) & \text{otherwise} \end{cases}$$

It was also determined independently by Hanani [28] using group divisible designs and incomplete covers

For $k = 4$ $C(k\ \lambda\ v)$ is known (cf [1] [32] [52] and [53]) to meet the Schonheim lower bound except for the following four values of $v$ (all with $\lambda = 1$) in which case Mills [52] [53] showed that

$$C(4\ 1\ v) = \begin{cases} \alpha(4\ 1\ v) + 1 & \text{if } v = 7\ \ 9\ \ 10 \\ \alpha(4\ 1\ v) + 2 & \text{if } v = 19 \end{cases}$$

The bound for $v = 19$ was obtained with the help of a computer [53]

For $k = 5$ the determination of covering number is still incomplete For $\lambda = 1$ the smallest value of $v$ for which $C(5\ 1\ v)$ is still unknown is $v = 28$ For results on covering of pairs by quintuples see [3]-[5], [26] [43] [56] [58] [59] and [62] For an excellent survey on these topics see [57]

Few results are known for the case $k \geq 6$ In [31] Honkala has proved a general result (with $\lambda = 1$) for the covering number with certain condition on $v$ It is shown that $C(k\ 1\ v) > \alpha(k\ 1,v)$ for large $k$ The following result of Honkala shows that Schonheim lower bound can be improved by 2 or more in many cases for $\lambda = 1$

**Theorem 2 2 3** [31] Suppose $t \geq 2$, $k \geq 2$ and $s \leq t$ are integers and $\iota = 0$

or 1 Denote $\beta = \lceil (s - 1 + 1)/(t - 1) \rceil$ Then

$$C(k, 1, t(k-1)+1) \geq t^2 + s$$

if $$k > \max \left\{ t + 1 - 1 + \beta, \frac{2t^2 + t(\beta-2)}{t + 1 - s} \right\}$$

Since $\alpha(k, 1 \quad t(k-1)+1) = \lceil t^2 + t(1-t)/k \rceil \leq t^2$ the above result shows that for large enough k the difference $C(k\ 1\ v) - \alpha(k\ 1,v)$ assumes large values

In [28], Hanani has proved the following theorem which improves Schonheim lower bound by 1 in certain general situations

**Theorem 2 2 4** [28] Let $(X\ \mathcal{B})$ be a covering design AD[k,λ,v] If $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ and if $\lambda v(v-1)/(k-1) \equiv -1 \pmod{k}$ then

$$C(k\ \lambda,v) \geq \alpha(k,\lambda,v) + 1$$

Using a simple counting argument, we give below an alternative proof for the above theorem Our proof is extendable to two other general situations

Let $(X,\mathcal{B})$ be a covering design AD[k λ v] For each $x \in X$, let $f(x)$ denote the number of blocks in $\mathcal{B}$ that contain x Since there are exactly (v-1) distinct pairsets of X containing x and a block, that contains x can cover (k-1) of these pairsets

$$f(x) \geq \left\lceil \frac{\lambda(v-1)}{k - 1} \right\rceil \equiv m \text{ (say)}$$

If $f(x) = \lambda(v-1)/(k-1)$ then every pairset containing x is covered exactly λ times let $g(x) = f(x) - m \geq 0$ Then the following Lemma is immediate

**Lemma 2 2 5** Let $(X,\mathcal{B})$ be a covering design AD[k,λ,v] and $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ If $\{x,y\} \subset X$ and $g(x) = 0$ or $g(y) = 0$ then $\{x,y\}$ is contained in exactly λ blocks

**Lemma 2 2 6** Let $(X,\mathcal{B})$ be a covering design AD[k λ,v] and $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ If $\sum_{x\in X} g(x) > 0$ then $\sum_{x\in X} g(x) \geq 2$

**Proof** Let $a \in X$ such that $g(a) > 0$ Hence there exists a pairset $\{a\ b\} \subset X$ which is contained in more than λ blocks Therefore $g(b) > 0$ and hence $\sum_{x\in X} g(x) \geq 2$ ■

**Proof of Theorem 2 2 4** If possible, suppose $C(k,\lambda,v) = \alpha(k\ \lambda\ v)$ By the hypothesis

$$\alpha(k,\lambda,v) = \frac{\lambda v(v-1) + (k-1)}{k(k-1)}$$

Now

$$\sum_{x\in X} g(x) = \sum_{x\in X} f(x) - vm$$

$$= k\ \alpha(k\ \lambda\ v) - \frac{\lambda v(v-1)}{k-1}$$

$$= 1 > 0$$

which is not possible from the above Remark 2 2 6 ■

**Lemma 2 2 7** Let v, k and λ be positive integers with $v > k \geq 3$ If $(X,\mathcal{B})$ is a covering design AD[k,λ,v] such that $\lambda(v-1) \equiv 0 \pmod{(k-1)}$, $\lambda v(v-1)/(k-1) \equiv -2 \pmod{k}$ and $|\mathcal{B}| = \alpha(k,\lambda,v)$ then there exists a unique pairset $\{a,b\} \subseteq X$ which is contained in exactly $(k+\lambda-1)$ blocks of $\mathcal{B}$ and every other pairset of X is contained in exactly λ blocks of $\mathcal{B}$

**Proof** From the hypothesis we have

$$\alpha(k\ \lambda,v) = \frac{\lambda v(v-1) + 2(k-1)}{k(k-1)} \qquad (2\ 38)$$

by (2 37) For any element $x \in X$ let f(x) be the number of blocks in $\mathcal{B}$ that contain x Since there are exactly (v-1) distinct pairs of X that contain x and since a given block of $\mathcal{B}$ contains at most (k-1) of them, we have $f(x) \geq \lambda(v-1)/(k-1)$ Clearly $f(x) > \lambda(v-1)/(k-1)$ if and only if there is a pair containing x that is contained in more than λ blocks of $\mathcal{B}$ Now

$$\sum_{x \in X} f(x) = k\,\alpha(k\,\lambda,v) = 2 + \lambda v(v-1)/(k-1) \qquad (2\,39)$$

by (2 38) Hence there is at least one pairset that is contained in more than $\lambda$ blocks of $\mathcal{B}$ Let {a b} be such a pairset Then we have

$$f(a) \geq 1 + \lambda(v-1)/(k-1), \qquad f(b) \geq 1 + \lambda(v-1)/(k-1)$$

and $f(x) \geq \lambda(v-1)/(k-1)$ for $x \in X$ $x \notin \{a,b\}$ Since (2 39) holds we must have

$$f(a) = f(b) = 1 + \lambda(v-1)/(k-1)$$

and $f(x) = \lambda(v-1)/(k-1)$ for $x \in X$ $x \notin \{a\ b\}$ Therefore {a b} is the only pairset that is contained in more than $\lambda$ blocks of $\mathcal{B}$ Since each block of $\mathcal{B}$ contains $\binom{k}{2}$ distinct pairs and there are $\alpha(k\ \lambda\ v)$ blocks in $\mathcal{B}$ the total number of pairs that is contained in blocks of $\mathcal{B}$ is

$$\frac{k(k-1)}{2}\,\alpha(k\ \lambda\ v) = \frac{\lambda v(v-1)}{2} + (k-1)$$

by (2 38) Hence {a b} will occur (k-1) extra times i e {a b} is contained in ($\lambda$+k-1) blocks of $\mathcal{B}$ and all other pairsets of X is contained in exactly $\lambda$ blocks of $\mathcal{B}$ ∎

For $\lambda = 1$ the following two corollaries (originally due to Fort and Hedlund [21] and Mills [53]) are a special case of Lemma 2 2 7

**Corollary 2 2 8** [21 Theorem 4] If $v = 6t + 5$ and $\mathcal{B}$ is a collection of $\alpha(3\ 1,v)$ triples that covers all the pairs of a set X of order v then there is one pair that occurs three times in these triples while all other pairs occur exactly once

**Corollary 2 2 9** [53 Theorem 5] If $v \equiv 7$ or 10 (mod 12) and if $\mathcal{B}$ is a collection of $\alpha(4\ 1\ v)$ quadruples that covers all pairs of a set X of order v, then there is one pair that occurs four times in these quadruples while all other pairs occur exactly once

**Theorem 2 2 10** Let $\lambda$ v and k be positive integers $v > k \geq 3$ $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ and let $\lambda v(v-1)/(k-1) \equiv -2 \pmod{k}$ If $\lambda(v-1)/(k-1) < \lambda + k - 2$ then $C(k\ \lambda\ v) \geq \alpha(k\ \lambda\ v) + 1$

**Proof** Suppose $(X\ \mathcal{B})$ is a covering design AD[k $\lambda$ v] such that $|\mathcal{B}| = \alpha(k,\lambda\ v)$ By Lemma 2 2 7 there exists a unique pairset say $\{a\ b\} \subseteq X$ which is contained in exactly $\lambda + k - 1$ blocks of $\mathcal{B}$ Following the same argument as in the proof of Lemma 2 2 7 the number of blocks of $\mathcal{B}$ that contains a f(a) is $\lambda(v-1)/(k-1) + 1$ Hence

$$f(a) = \lambda(v-1)/(k-1) + 1 \geq \lambda + k - 1,$$

a contradiction Thus the result follows ■

For $\lambda = 1$ Theorem 2 2 10 gives the following corollary

**Corollary 2 2 11** Let $k \geq 4$ be a positive integer then $C(k\ 1,2k-1) \geq \alpha(k\ 1\ 2k-1) + 1 = 5$

As a consequence of Corollary 2 2 11 C(4,1 7) $\geq$ 5 [53] C(5 1 9) $\geq$ 5 [54] etc

**Lemma 2 2 12** Let v k and $\lambda$ be positive integers with $v > k \geq 4$ If $(X,\mathcal{B})$ is a covering design AD[k $\lambda$ v] such that $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ $\lambda v(v-1)/(k-1) \equiv -3 \pmod{k}$ and $|\mathcal{B}| = \alpha(k\ \lambda\ v)$ then there exists three pairsets $\{s\ t\}$ $\{t\ u\}$ $\{u\ s\}$ of $\lambda$ which are contained in exactly $\lambda + \frac{1}{2}(k-1)$ blocks of $\mathcal{B}$ and every other pairsets of X is contained in exactly $\lambda$ blocks of $\mathcal{B}$

**Proof** By the hypothesis and (2 37)

$$\alpha(k,\lambda\ v) = \frac{\lambda v(v-1) + 3(k-1)}{k(k-1)} \qquad (2\ 40)$$

For any element $x \in \lambda$ let f(x) be the number of blocks in $\mathcal{B}$ that contain x Since there are exactly (v-1) distinct pairs of X that contain x and since a given block contains at most k - 1 of them we have $f(x) \geq \lambda(v-1)/(k-1)$

Clearly $f(x) > \lambda(v-1)/(k-1)$ if and only if there is a pair containing $x$ that is contained in more than $\lambda$ blocks of $\mathcal{B}$ Now

$$\sum_{x \in X} f(x) = k\ \alpha(k\ 1\ v) = 3 + \lambda v(v-1)/(k-1) \qquad (2\ 41)$$

by (2 40) Hence there is at least one pairset that is contained in more than $\lambda$ blocks of $\mathcal{B}$ Let $\{s\ t\}$ be such a pairset Then we have

$$f(s) \geq 1 + \lambda(v-1)/(k-1), \qquad f(t) \geq 1 + \lambda(v-1)/(k-1)$$

and $f(x) \geq \lambda(v-1)/(k-1)$ for $x \in X$ $x \notin \{s\ t\}$ Observe that

$$\binom{k}{2}\ \alpha(k\ \lambda\ v) = \frac{\lambda v(v-1)}{2} + \frac{3}{2}(k-1) \qquad (2\ 42)$$

by (2 40) If $f(s) = 2 + \lambda(v-1)/k-1$ $f(t) = 1 + \lambda(v-1)/(k-1)$ and $f(x) = \lambda(v-1)/(k-1)$ $x \in X$ $x \notin \{s\ t\}$ then by (2 42) and Lemma 2 2 5 the pairset $\{s\ t\}$ will be contained in $\lambda + \frac{3}{2}(k-1)$ blocks of $\mathcal{B}$ and all other pairsets of $X$ will be contained in exactly $\lambda$ blocks of $\mathcal{B}$ i e $f(s) = f(t)$ a contradiction Hence there exists $u \in X$ $u \notin \{s\ t\}$ such that

$$f(s) = f(t) = f(u) = 1 + \lambda(v-1)/(k-1)$$

and $f(x) = \lambda(v-1)/(k-1)$ for $x \in X$ $x \notin \{s\ t\ u\}$ Hence by Lemma 2 2 5 the pairs which are contained in more than $\lambda$ blocks of $\mathcal{B}$ will contain only the elements of the set $\{s\ t\ u\}$ Since $f(s) = f(t) = f(u)$ each of the pairsets $\{s\ t\}$ $\{t\ u\}$ and $\{s\ u\}$ will occur in extra equal number of times i e the pairsets $\{s\ t\}$ $\{t\ u\}$ and $\{u\ s\}$ will be contained in exactly $\lambda + \frac{1}{2}(k-1)$ blocks of $\mathcal{B}$ and all other pairset of $X$ will be contained in exactly $\lambda$ blocks of $\mathcal{B}$ ■

**Theorem** 2 2 13 Let $\lambda$ $v$ and $k$ be positive integers, $v > k \geq 4$ $\lambda(v-1) \equiv 0 \pmod{(k-1)}$ and let $\lambda v(v-1)/(k-1) \equiv -3 \pmod{k}$ If $\lambda(v-1)/(k-1) < \lambda + \frac{1}{2}(k-3)$ then $C(k\ \lambda\ v) \geq \alpha(k\ \lambda\ v) + 1$

**Proof** Suppose $(X\ \mathcal{B})$ is a covering design AD[k,λ,v] such that $|\mathcal{B}| = \alpha(k\ \lambda\ v)$ By Lemma 2 2 12 there exists a pairset $\{s\ t\} \subseteq X$ which is

contained in exactly $\lambda + \frac{1}{2}(k-1)$ blocks of $\mathcal{B}$ Following the argument as in the proof of 2 2 12 the number of blocks of $\mathcal{B}$ that contains s f(s) is $\lambda(v-1)/(k-1) + 1$ Hence

$$f(s) = \lambda(v-1)/(k-1) + 1 \geq \lambda + \frac{1}{2}(k-1)$$

a contradiction Thus the result follows ■

For the sake of completeness we give the table for C(k 1 v) from [14]

Table 2 1 Bounds on C(k 1,v)

| $v$ \ $k$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 1 | | | | | | | | | |
| 4 | 3 | 1 | | | | | | | | |
| 5 | 4 | 3 | 1 | | | | | | | |
| 6 | 6 | 3 | 3 | 1 | | | | | | |
| 7 | 7 | 5 | 3 | 3 | 1 | | | | | |
| 8 | 11 | 6 | 4 | 3 | 3 | 1 | | | | |
| 9 | 12 | 8 | 5 | 3 | 3 | 3 | 1 | | | |
| 10 | 17 | 9 | 6 | 4 | 3 | 3 | 3 | 1 | | |
| 11 | 19 | 11 | 7 | 6 | 4 | 3 | 3 | 3 | 1 | |
| 12 | 24 | 12 | 9 | 6 | 5 | 3 | 3 | 3 | 3 | 1 |
| 13 | 26 | 13 | 10 | 7 | 6 | 4 | 3 | 3 | 3 | 3 |
| 14 | 33 | 18 | 12 | 7 | 6 | 5 | 4 | 3 | 3 | 3 |
| 15 | 35 | 19 | 13 | 10 | 7 | 6 | 4 | 3 | 3 | 3 |
| 16 | 43 | 20 | 15 | 10 | 8 | 6 | 5 | 4 | 3 | 3 |
| 17 | 46 | 26 | 16 | 12 | 9 | 7 | 6 | 5 | 4 | 3 |
| 18 | 54 | 27 | 18 | 12 | 10 | 7 | 6 | 5 | 4 | 3 |
| 19 | 57 | 31 | 19 | 14–15 | 11 | 9 | 7 | 6 | 5 | 4 |
| 20 | 67 | 35 | 21 | 16 | 12 | 9 | 7 | 6 | 6 | 4 |
| 21 | 70 | 37 | 21 | 17 | 13 | 11 | 7 | 7 | 6 | 5 |
| 22 | 81 | 39 | 27 | 19 | 13 | 11 | 9 | 7 | 6 | 6 |
| 23 | 85 | 46 | 28 | 20–21 | 15–16 | 12 | 10 | 8 | 7 | 6 |
| 24 | 96 | 48 | 30 | 21–22 | 17 | 12 | 11 | 8 | 7 | 6 |
| 25 | 100 | 50 | 30 | 23 | 18 | 13 | 11 | 10 | 7 | 7 |
| 26 | 113 | 59 | 37 | 24 | 19–20 | 13 | 12 | 10 | 8 | 7 |
| 27 | 117 | 61 | 38 | 27 | 20 | 16–17 | 12 | 11 | 9 | 7 |
| 28 | 131 | 63 | 40–43 | 28 | 21–22 | 17–18 | 13–14 | 11 | 10 | 7 |
| 29 | 136 | 73 | 42–44 | 29–31 | 22–24 | 18 | 14 | 12 | 10 | 9 |
| 30 | 150 | 75 | 48 | 31 | 24–25 | 19 | 15 | 13 | 11 | 9 |
| 31 | 155 | 78 | 50 | 31 | 26 | 20 | 15–18 | 13 | 12 | 10 |
| 32 | 171 | 88 | 52–54 | 38 | 28–31 | 20 | 15–19 | 13–15 | 12 | 10 |

# CHAPTER III

# GROUP DIVISIBLE DESIGNS AND GROUP COVERING DESIGNS

In the first section of this chapter, a few results are established on group divisible designs. Those include a stronger necessary condition for the existence of group divisible designs (analogous to the **Fisher's Inequality** for BIBD's). In the next section we introduce a new combinatorial design called **group covering design** and establish many results on these designs. These are used in the Chapter V of the dissertation to further improve the existing lower bounds on $K_q(n, R)$ $q \geq 3$.

## 3.1 Group Divisible Designs

Let $k$, $m$, $\lambda$ and $v$ be positive integers. A triple $(X, \mathcal{G}, \mathcal{B})$ where $X$ is a finite set of points, $\mathcal{G}$ is a family of pairwise disjoint nonempty subsets of $X$ (called *groups*) whose union is $X$, and $\mathcal{B}$ is a collection of subsets of $X$ (called *blocks*) is called a *group divisible design* denoted by $GD[k, \lambda, m, v]$ if

(i) $|X| = v$

(ii) $|G_i| = m$ for every $G_i \in \mathcal{G}$

(iii) $|B_j| = k$ for every $B_j \in \mathcal{B}$

(iv) $|G_i \cap B_j| \leq 1$ for every $G_i \in \mathcal{G}$ and $B_j \in \mathcal{B}$

(v) Every pairset $\{x, y\} \subseteq X$ such that $x$ and $y$ belong to distinct groups is contained in exactly $\lambda$ blocks of $\mathcal{B}$.

When $|X| = km$, $GD[k, \lambda, m, km]$ is called a *transversal design*, denoted by

TD[k λ m] Thus each block is a *transversal* of the groups as each block contains precisely one element from each group

It follows immediately that a GD[k λ 1 v] is a B$^1$BD[k λ v]

Following notations of Hanani [28] the set of integers v for which group divisible designs GD[k λ m v] exist is denoted by GD(k λ m) Clearly GD(k λ m) ⊆ mI where I is the set of positive integers The set of integers m for which transversal designs TD[k λ m] exist is denoted by TD(k λ)

However when λ = 1 one usually represents GD[k,λ m v] TD[k λ m] GD(k λ m) and TD(k λ) respectively by GD[k m v], TD[k m] GD(k m) and TD(k)

The existence of a GD[k λ m v] was first discussed in [28] A necessary condition for the existence of a group divisible design is given by the following theorem

**Theorem** 3 1 1 [28] If a group divisible design GD[k λ m v] exists then

$$v \equiv 0 \pmod{m} \qquad v \geq km \qquad \lambda(v-m) \equiv 0 \pmod{(k-1)}$$

and $\lambda v(v-m) \equiv 0 \pmod{k(k-1)}$

When v = km and λ = 1 Hanani has proved the following theorem

**Theorem** 3 1 2 [28] If m ∈ TD(k) and m > 1 then m ≥ k-1

Hence it follows immediately from the above theorem that if 1 < m < k-1 then a GD[k m km] does not exist Therefore the conditions of Theorem 3 1 1 are not sufficient for the existence of a GD[k λ m v] Further it has been already proved by Tary [75] that a GD[4 6 24] does not exist

However group divisible designs with block sizes 3 and 4 are known to exist (see e g [11], [28]) for all λ \ and m satisfying the necessary conditions of Theorem 3 1 1 with exceptions of GD[4 2,8] and GD[4 6 24] Very little is known for the case k ≥ 5 For k = 5 some special cases are considered by Assaf *et al* [3] and Avidan [6]

For $v > km$ and $\lambda = 1$ we prove the following stronger result for the existence of a group divisible design using the methodology of Wilson [84]

**Theorem 3 1 3** If there exists a group divisible design GD[k m v] with $v > km$ then $v \geq k(k-1) + m$

**Proof** Let $(X \mathcal{G} \mathcal{B})$ be a group divisible design GD[k m,v] Let B be a block of GD[k m,v] Then there exists a group $G_o \in \mathcal{G}$ such that $B \cap G_o = \phi$ Let $x_o \in G_o$ For any point $x \in B$, let $B_x$ be the block which contains the pairset $\{x_o\ x\}$ Then for any two distinct points x and y of B, $(B_x \setminus \{x_o\}) \cap (B_y \setminus \{x_o\}) = \phi$ For if $y_o \in B_x \cap B_y$, $y_o \neq x_o$, then $\{y_o\ x_o\} \subseteq B_x \cap B_y$, contradicting the fact that each pair is contained in exactly one block $B \in \mathcal{B}$ Also $(B_x \setminus \{x_o\}) \cap G_o = \phi$ for every $x \in B$ Thus the set $G_o \cup (\bigcup_{x \in B} B_x \setminus \{x_o\})$ contains $m + k(k-1)$ points and this number cannot exceed v ■

**Remark** If $m = 1$, the above theorem gives $v \geq k(k-1) + 1$, the famous *Fisher's inequality* for $\lambda = 1$ (Theorem 2 2 2)

As a corollary to Theorem 3 1 3 the nonexistence of the following group divisible designs follows immediately

**Corollary 3 1 4** GD[8,2 30], GD[8 2,44], GD[9,3,51] do not exist

Since the number of groups must be an integer, we have the following trivial result

**Corollary 3 1 5** If there exists a GD[k m v], $v > km$ and $m \nmid (k(k-1) + m)$ then $v \geq m\lceil (k(k-1)+m)/m \rceil$

**Theorem 3 1 6** Let C and D be two disjoint blocks in a GD[k,m v] and let $G_o$ be a group with $G_o \cap C = 1$ and $G_o \cap D = \phi$ Then $v \geq k^2 + m - 1$

**Proof** Let $G_o \cap C = \{x_o\}$ For each $x \in D$ let $B_x$ be the block which contains

the pairset $\{x\ x_o\}$ As in the proof of Theorem 3 1 3 $(B_x \setminus \{x_o\}) \cap (B_y \setminus \{x_o\}) = \phi$ for any two distinct points x and y of D Also for each $x \in D$ $(B_x \setminus \{x_o\}) \cap C = \phi$ For if this contains some point y then $\{y\ x_o\} \subseteq B_x \cap C$ contradicting the fact that each pairset is contained in exactly one block Also $(B_x \setminus \{x_o\}) \cap G_o = \phi$ for every $x \in D$ and $G_o \cap (C \setminus \{x_o\}) = \phi$ Thus the set $G_o \cup (C \setminus \{x_o\}) \cup (\bigcup_{x \in D} B_x \setminus \{x_o\})$ contains $m + (k-1) + k(k-1)$ points which is at most v Thus $v \geq k^2 + m - 1$ ■

Since any two distinct blocks in a group divisible design cannot intersect at more than one point we have the following obvious corollary

**Corollary** 3 1 7 Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group divisible design GD[k m v] with $v < k^2 + m - 1$ Let C and D be any two distinct blocks of $\mathcal{B}$ such that $C \cap G_1 = 1$ and $D \cap G_1 = \phi$ for some $G_1 \in \mathcal{G}$ Then C and D intersect at a point

For $k \geq 2$ and $v = k(k-1) + m$ the above corollary still holds Hence if C and D are any two distinct blocks of a BIBD B[k 1 k(k-1)+1] then we have the following corollary originally due to Wilson [84 p 226]

**Corollary** 3 1 8 Any two distinct blocks of a B[k 1 k(k-1)+1] intersect at a point

**Theorem** 3 1 9 If a transversal design TD[k m] contains two disjoint blocks then $m \geq k$

**Proof** Let $(X\ \mathcal{G}\ \mathcal{B})$ be a TD[k m] with $C,D \in \mathcal{B}$ such that $C \cap D = \phi$ Since each block is a transversal of the groups for any $G_o \in \mathcal{G}$ $G_o \cap C = \{x_o\}$ and $G_o \cap D = \{y_o\}$ For any point y $(\neq y_o)$ of D, let $B_y$ be the block which contains the pairset $\{x_o\ y\}$ As in the proof of Theorem 3 1 3 $(B_s \setminus \{x_o\}) \cap (B_t \setminus \{x_o\}) = \phi$ for any two distinct points s and t of D Also $G_o \cap (B_y \setminus \{x_o\}) = \phi$ and $(B_y \setminus \{x_o\}) \cap C = \phi$ for each $y(\neq y_o)$ of D

Hence, the set $G_o \cup (C\backslash\{x_o\}) \cup \left( \bigcup_{\substack{y\in D \\ y\neq y_0}} (B_y\backslash\{x_o\}) \right.$ contains $m + (k-1) + (k-1)(k-1)$ points and this number cannot exceed km Thus $m \geq k$ ■

In [28] Hanani has shown that the above condition of Theorem 3 1 9 is sufficient for the existence of at least two disjoint blocks Hence we have the following corollary

**Corollary** 3 1 10 In a transversal design TD[k m] there are at least two disjoint blocks *if and only if* $m \geq k$

Hence if $m = k-1$ then any two distinct blocks of TD[k m] have exactly one point of intersection reproving the following result [78, p 192]

**Theorem** 3 1 11 The intersection of any two distict blocks in a transversal design TD[m+1,m] contains exactly one element

The following two results are known

**Theorem** 3 1 12 [28 Lemma 3 5] For every prime power q $q \in TD(q+1)$ In other words TD[q+1 1 q] exists for every prime power q

**Theorem** 3 1 13 [28 Lemma 2 12] There exists a group divisible design GD[k k-1 v] if and only if there exists a BIBD B[k 1 v+1]

**Theorem** 3 1 14 Let m n and t be positive integers $t \geq n \geq 3$ If there exists a transversal design TD[n m] and a group divisible design GD[n,(n-1)m (n-1)mt] then the group divisible design GD[n m m(t(n-1)+1)] exists

**Proof** For each j = 1 2 t let $(X_j, \mathcal{G}_j, \mathcal{P}_j)$ be a transversal design TD[n m] such that a particular group $G_o$ belongs to all $\mathcal{G}_j$'s and all other groups are pairwise disjoint In other words $\mathcal{G}_j = \{G_o, G_{j1}, G_{j2}, \ldots, G_{j(n-1)}\}$, where for all j and $\ell$ $1 \leq j \leq t$ and $1 \leq \ell \leq n-1$ $G_o$ and $G_{j\ell}$ are pairwise

disjoint groups Let $Y = \bigcup_{j=1}^{t} \bigcup_{\ell=1}^{n-1} G_{j\ell}$ $\mathcal{G} = \{ \bigcup_{\ell=1}^{n-1} G_{j\ell} \quad 1 \le j \le t \}$ Then $|Y| =$ $(n-1)mt$ $|\mathcal{G}| = t$ and each group in $\mathcal{G}$ has cardinality $(n-1)m$ Hence by hypothesis there exists a collection $\mathcal{P}$ of n-subsets such that $(Y\ \mathcal{G}\ \mathcal{P})$ is a group divisible design $GD[n\ (n-1)m\ (n-1)mt]$ It is now easy to verify that $(X\ \mathcal{H}\ \mathcal{B})$ is a group divisible design $GD[n\ m\ (t(n-1)+1)m]$ where $X = Y \cup G_o$ $\mathcal{H} = \{G_{j\ell} \quad 1 \le j \le t \quad 1 \le \ell \le n-1\} \cup \{G_o\}$ and $\mathcal{B} = \mathcal{P} \cup \mathcal{P}_1 \cup \quad \cup \mathcal{P}_t$ ■

**Corollary 3 1 15** Let m be a prime power such that $m = n - 1 \ge 2$ and let $t \ge n$ If there exists a group divisible design $GD[m+1\ m^2\ tm^2]$ then there exists a BIBD $B[m+1\ 1\ m(tm+1)+1]$

**Proof** Since m is a prime power there exists a transversal design $TD[m+1\ m]$ by Theorem 3 1 12 Hence there exists a group divisible design $GD[m+1\ m\ m(tm+1)]$ by Theorem 3 1 14 and the result follows from Theorem 3 1 13 ■

**Note** Let $m = n - 1 \ge 2$ be a prime power If $t = n = m + 1$ and there exists a $TD[m+1\ m^2]$ then there exists a $BIBD[m+1\ 1\ m(m^2+m+1)+1]$

## 3 2 Group Covering Designs

In the previous section we have dealt with group divisible designs and observed that such designs do not always exist To deal with such cases the notion of *group covering designs* analogous to covering designs is introduced in this section The study of group covering designs apart from being a generalisation of covering designs finds applications in q-ary covering codes $q \ge 3$ It will be discussed in detail in Chapter V of this thesis In [69] Sloane has discussed a particular case of these designs which have application in switching networks

Zhang [88] and Honkala [31] have studied the covering design problem to improve the lower bounds for binary covering codes In [12] Chen and

Honkala have studied a local covering problem to give better bounds for q-ary covering codes ($q \geq 3$) This class of local covering problem is classified as a group covering design and many results analogous to results for covering designs are obtained Exact bounds for many classes of group covering designs are also found

### 3 2 1 Preliminary results and lower bounds on G(k,m,n)

**Definition** Let m n and k be positive integers with $n \geq k \geq 2$ A triple $(X\ \mathcal{G}\ \mathcal{B})$ where X is a finite set of points $\mathcal{G}$ is a family of pairwise disjoint nonempty subsets (called *groups*) of X whose union is X and $\mathcal{B}$ is a collection of subsets of X (called *blocks*) is a *group covering design* denoted by GC[k,m nm] if

(i) $|X| = nm$

(ii) $|\mathcal{G}| = n$ and $|G_i| = m$ for every $G_i \in \mathcal{G}$

(iii) $|B_j| = k$ for every $B_j \in \mathcal{B}$

(iv) $|G_i \cap B_j| \leq 1$ for every $G_i \in \mathcal{G}$ and every $B_j \in \mathcal{B}$

(v) Every pairset $\{x\ y\} \subset X$ such that x and y belong to distinct groups is contained in *at least* one block of $\mathcal{B}$

Throughout the chapter the members of a pairset are assumed to belong to distinct groups It follows immediately that AD[k 1 n] is a group covering design GC[k 1 n ] Henceforth we will denote a group covering design GC[k m nm] by GC[k m n]

A GC[k m n] with b blocks is said to be *minimum* if for any GC[k m n] with b blocks one always has $b \leq b'$ The number b for a minimum group covering design GC[k m,n] is called a *group covering* number denoted by G(k m n) Suppose m n and k are positive integers such that a GC[k m n] exists Then there are $\binom{n}{2}$ distinct pair of groups, and each pair of groups has $m^2$ distinct pairsets $\{x,y\}$ such that x and y are from distinct

groups Since each block in $\mathcal{B}$ contains $\binom{k}{2}$ distinct pairsets we have the following trivial lower bound for G(k m n)

$$G(k\ m\ n) \geq \frac{n(n-1)}{k(k-1)}\ m^2 \qquad (3\ 1)$$

Equality in (3 1) exists if there exists a GD[k,m nm] Analogous to Schonheim lower bound for covering designs the following theorem gives a better lower bound

**Theorem** 3 2 1 Let k n and m be positive integers with $n \geq k \geq 2$ Then

$$G(k\ m\ n) \geq \left\lceil \frac{mn}{k} \left\lceil \frac{m(n-1)}{k-1} \right\rceil \right\rceil \equiv \beta(k\ m\ n) \quad \text{(say)} \qquad (3\ 2)$$

**Proof** Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design GC[k m n] Let $x_o \in X$ Then the number of pairsets $\{x_o\ y\}$ is m(n-1) If $B_o \in \mathcal{B}$ is a block containing $x_o$ then $B_o$ can cover (k-1) of these pairsets $\{x_o\ y\}$ Hence the replication number of every point i e the number of blocks containing the point in the group covering design is at least $\lceil m(n-1)/(k-1) \rceil$ Since there are n groups each having m points and each block has size k a simple counting argument gives

$$k\ G(k\ m\ n) \geq mn \lceil m(n-1)/(k-1) \rceil$$

As G(k m n) is an integer the result follows ∎

**Remark** AD[k 1 n] is also a group covering design GC[k 1 n] Thus

$$C(k\ 1\ n) = G(k\ 1\ n) \geq \left\lceil \frac{n}{k} \left\lceil \frac{n\ -\ 1}{k\ -\ 1} \right\rceil \right\rceil$$

which is the best known lower bound for C(k 1 n) [68]

A similar result was proved by Chen and Honkala [12] while estimating the minimum number of (R+2)-weight codewords required to cover all the 2-weight words of any q-ary covering code of length n and covering radius R

If a group divisible design GD[k m nm] exists then k, m and n must

satisfy the necessary condition of Theorem 3 1 1 and hence the number of blocks is $\frac{n(n-1)}{k(k-1)}\, m^2$ This observation gives the following

**Theorem** 3 2 2 Let k m and n satisfy the necessary condition of Theorem 3 1 1 If a group divisible design GD[k m nm] does not exist then

$$G(k\ m\ n) \geq \frac{n(n-1)}{k(k-1)}\, m^2 + 1$$

In particular when $n = k$ and $1 < m < k - 1$ by Theorem 3 1 2 the following useful corollary is immediate

**Corollary** 3 2 3 Let k and m be positive integers and let $1 < m < k - 1$ Then $G(k\ m\ k) \geq m^2 + 1$

Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design GC[k m n] and let $x_o \in X$ Then the number of pairsets $\{x_o\ y\}$ is $m(n-1)$ If $B_o \in \mathcal{B}$ is a block containing $x_o$ then $B_o$ can cover $(k-1)$ of these pairset $\{x_o\ y\}$ Thus the number of blocks that contain $x_o$ denoted by $f(x_o)$ is at least $\lceil m(n-1)/(k-1) \rceil$ Hence

$$f(x_o) \geq \left\lceil \frac{m(n-1)}{(k-1)} \right\rceil \equiv m_o \quad \text{(say)}$$

Let $g(x_0) = f(x_0) - m_o \geq 0$ If $g(x_o) > 0$ and $m(n-1) \equiv 0 \pmod{k-1}$ then there exists at least one pairset $\{x_o\ y\}$ which is contained in two or more blocks Thus if $g(x_o) = 0$ then every pairset $\{x_o, y\}$ will occur in exactly one block This proves the following lemma

**Lemma** 3 2 4 Let $(X, \mathcal{G}, \mathcal{B})$ be a group covering design GC[k,m,n] and let $\{x\ y\} \subset X$ be a pairset If either $g(x) = 0$ or $g(y) = 0$ and $m(n-1) \equiv 0 \pmod{(k-1)}$ then $\{x\ y\}$ is contained in exactly one block of the group covering design

The following theorem is analogous to Theorem 2 2 4

**Theorem** 3 2 5 Let $(X\ \mathcal{G}, \mathcal{B})$ be a group covering design GC[k m n] If

$m(n-1) \equiv 0 \pmod{(k-1)}$ and $nm^2(n-1)/(k-1) \equiv -1 \pmod{k}$ then $G(k,m\ n) \geq \beta(k\ m,n) + 1$

**Proof** If possible suppose $G(k\ m\ n) = \beta(k\ m\ n)$ By the hypothesis $\beta(k,m\ n) = (nm^2(n-1)+(k-1))/k(k-1)$ Now

$$\sum_{x \in \setminus} g(x) = \sum_{x \in X} f(x) - \sum_{x \in X} m_o$$
$$= k\ \beta(k\ m\ n) - nm^2(n-1)/(k-1) = 1$$

So there exists a unique $x_o \in X$ such that $g(x_o) = 1$ and $g(x) = 0$ for $x \neq x_o$ Hence by Lemma 3 2 4 every pairset $\{x_o\ y\}$ must be contained in exactly one block of $\mathcal{B}$ But since $g(x_o) = 1 > 0$ there exists a pairset $\{x_o\ u\}$ which will be contained in at least two blocks a contradiction ■

As a corollary to the above theorem the following improvements to (3 2) is immediate

**Corollary** 3 2 6 $G(7\ 2\ 13) \geq 16$ $G(7\ 2\ 16) \geq 24$ $G(5,4\ 8) \geq 46$

$G(5,4\ 13) \geq 126$ $G(11\ 4\ 16) \geq 36$ $G(5\ 4\ 18) \geq 246$

**Lemma** 3 2 7 Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design $GC[k\ m\ n]$ and let $m(n-1) \equiv 0 \pmod{(k-1)}$ and $nm^2(n-1)/(k-1) \equiv -2 \pmod{k}$ If $G(k\ m\ n) = \beta(k,m\ n)$ then there exists a unique pairset $\{x_0\ y_0\} \subseteq \setminus$ which is contained in exactly k blocks of $\mathcal{B}$ and every other pairset $\{x\ y\} \subseteq X$ is contained in exactly one block of $\mathcal{B}$

**Proof** From the hypothesis $G(k,m,n) = \dfrac{nm^2(n-1) + 2(k-1)}{k(k-1)}$ Also

$$\sum_{x \in X} g(x) = \sum_{x \in X} f(x) - \sum_{x \in X} m_o$$
$$= k\ \beta(k,m\ n) - nm^2(n-1)/(k-1) = 2$$

Thus there exists $x_o \in X$ such that $g(x_o) > 0$ Hence there exists $y_o \in \setminus$ such that $\{x_o\ y_o\}$ is contained in at least two blocks say, $B_1 = \{x_o\ y_o\ y_1$ $y_{k-2}\}$, $B_2 = \{x_o\ y_o, z_1\ z_2,\ z_{k-2}\}$ Since $y_o$ is contained in $m(n-1)$

distinct pairsets $\mathcal{B}$ must contain at least $\ell_0 = \left\lceil \frac{m(n-1) - 1 - 2(k-2)}{k-1} \right\rceil$ more blocks each containing $y_0$ Thus $f(y_0) \geq \ell_0 + 2 = m_0 + 1$ So $g(y_0) \geq 1$ Hence $g(x_0) = g(y_0) = 1$ and $g(x) = 0$ for all $x \notin \{x_0\ y_0\}$ Hence by Lemma 3 2 4, every pairset having at most one element from $\{x_0\ y_0\}$ will be contained in exactly one block Since each block contains $\binom{k}{2}$ pairsets and $\frac{k(k-1)}{2}\beta(k\ m\ n) = \frac{nm^2(n-1)}{2} + (k-1)$ the pairset $\{x_0\ y_0\}$ will be contained in exactly k blocks ■

**Theorem** 3 2 8 Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design GC[k m n] and let $m(n-1) \equiv 0 \pmod{(k-1)}$ and $nm^2(n-1)/(k-1) \equiv -2 \pmod{k}$ If $m(n-1)/(k-1) < k + m - 2$ then $G(k\ m\ n) \geq \beta(k\ m\ n) + 1$

**Proof** Suppose $G(k\ m\ n) = \beta(k\ m\ n)$ By Lemma 3 2 7 there exists a pairset $\{x_0\ y_0\}$ which is contained in exactly k blocks of $\mathcal{B}$ $f(x_0) = m_0 + 1$ and $f(y_0) = m_0 + 1$ Let $y_0 \in G_0$ Then for every $y \in G_0$ $y \neq y_0$ the pairset $\{x_0, y\}$ must be contained in exactly one block of $\mathcal{B}$ Thus $f(x_0) = m_0 + 1 \geq k + (m-1)$ a contradiction ■

As a consequence of the above theorem the following improvements to (3 2) is immediate

**Corollary** 3 2 9 $G(6\ 2,11) \geq 16$ $G(8,3\ 15) \geq 35$, $G(5\ 4,7) \geq 35$, $G(10,4\ 19) \geq 62$

**Lemma** 3 2 10 Let m n and k be positive integers with $n \geq k > 3$ and let $(X,\mathcal{G},\mathcal{B})$ be a group covering design GC[k,m n] If $m(n-1) \equiv 0 \pmod{(k-1)}$ $nm^2(n-1)/(k-1) \equiv -3 \pmod{k}$ and $G(k\ m,n) = \beta(k,m,n)$ then there exists three elements $x_0$, $y_0$ and $z_0$ of X belonging to distinct groups such that each of the pairsets $\{x_0,y_0\}$ $\{y_0\ z_0\}$ and $\{z_0\ x_0\}$ is contained in $\frac{1}{2}(k+1)$ blocks of $\mathcal{B}$ and all other pairsets are contained in exactly one block

**Proof** By the hypothesis, $G(k\ m,n) = (nm^2(n-1) + 3(k-1))/(k(k-1))$ Also

$$\sum_{x\in X} g(x) = \sum_{x\in X} f(x) - \sum_{x\in X} m_o$$

$$= k\ \beta(k\ m\ n) - nm^2(n-1)/(k-1) = 3$$

Thus, there exists a point $x_o \in X$ such that $g(x_o) > 0$ Following the same argument as in Lemma 3 2 7 there exists $y_o \in X$ such that $g(y_o) > 0$ and $x_o$ and $y_o$ are in two distinct groups Observe that

$$\frac{k(k-1)}{2}\ \beta(k\ m\ n) = \frac{nm^2(n-1)}{2} + \frac{3}{2}\ (k-1)$$

If $g(x_o) = 2$ and $g(y_o) = 1$ then $g(x) = 0$ for all $x \notin \{x_o\ y_o\}$ Following the same argument as in Lemma 3 2 7 $\{x_o\ y_o\}$ will be contained in $\frac{3}{2}(k-1) + 1$ blocks of $\mathcal{B}$ and all other pairsets $\{x\ y\}$ will be contained in exactly one block of $\mathcal{B}$ Hence $g(x_o) = g(y_o)$ a contradiction Hence $g(x_o) = 1$ and $g(y_o) = 1$ So there exists $z_o \in X$ such that $g(z_o) = 1$ Then there will be (k-1) pairsets containing $x_o$ (k - 1) pairsets containing $y_o$ and (k-1) pairsets containing $z_o$ (not necessarily distinct) which are contained in more than one block Since $g(x) = 0$ for $x \notin \{x_o, y_o\ z_o\}$ by Lemma 3 2 4 the above (k-1) extra pairsets containing $x_o$ must contain either $y_o$ or $z_o$ Similarly for the pairsets containing $y_o$ and $z_o$ If $x_o$ and $z_o$ belong to the same group then the pairset $\{x_o\ y_o\}$ will occur exactly k-1 times extra So $z_o$ cannot be paired with $y_o$ a contradiction Hence, $x_o$ $y_o$ and $z_o$ belong to distinct groups and each of the pairsets $\{x_o\ y_o\}$, $\{y_o, z_o\}$ and $\{z_o, x_o\}$ must occur (k-1)/2 times extra i e , the pairsets $\{x_o, y_o\}$ $\{y_o\ z_o\}$ and $\{z_o, x_o\}$ must occur in (k+1)/2 blocks and all other paisets of X will occur exactly once ■

Following the same argument as in the Theorem 3 2 8 we have the following result

**Theorem 3 2 11** Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design GC[k m n] and let $m(n-1) \equiv 0 \pmod{(k-1)}$ and $\frac{nm^2(n-1)}{k-1} \equiv -3 \pmod{k}$ If $\frac{m(n-1)}{k-1} < \frac{1}{2}(k-3) + m$ then $G(k\ m,n) \geq \beta(k,m,n) + 1$

The above theorem gives the following improvements to (3 2)

**Corollary 3 2 12** $G(7\ 2,10) \geq 10$ $G(9\ 2\ 13) \geq 10$

$G(11\ 2\ 16) \geq 10$ $G(9\ 4,13) \geq 36$

**Theorem 3 2 13** $G(5\ 2\ 7) \geq 10$

**Proof** Suppose $(X\ \mathcal{G},\mathcal{B})$ is a group covering design GC[5 2,7] with 9 blocks Let $\mathcal{G} = \{G_1,G_2, \ ,G_7\}$ For simplicity, let $G_1 = \{1,2\}$ meaning thereby that 1(2) represents the first (second) element of the group $G_1$ Moreover for B $\in \mathcal{B}$ (pairset P) it is convenient to write $B = x_1 \ x_7$ $(P = x_1 \ x_7)$ with $x_1 \in G_1 \cup \{\phi\}$ $x_1 = \phi$ means B(P) does not contain any element of $G_1$ Since $\beta(5\ 2,7) = 9$, by Lemma 3 2 10 there exists three pairsets, say, $P_1 = 11\phi \ \phi$ $P_2 = \phi 11\phi \ \phi$ and $P_3 = 1\phi 1\phi \ \phi$ that are contained in exactly 3 blocks of $\mathcal{B}$ and every other pairset is contained in exactly 1 block Following the same argument as in Lemma 3 2 10 it is easy to see that for each $i \in \{1\ 2\ 3\}$ there exists exactly 4 blocks having $x_1 = 1$ Since each fo the pairsets $12\phi \ \phi$, $21\phi \ \phi$ and $22\phi \ \phi$ occurs in exactly 1 block, there exists 6 blocks $B_1, \ , B_6$ whose first 2 entries are 11, 11 11 12, 21 and 22 respectively Since each of the pairsets $P_2$ and $P_3$ occurs in exactly 3 blocks and $x_3 = 1$ for only 4 blocks, the following two possibilities arise

Case 1 $B_1 = 1\ 1\ 1\ ****$

$B_2 = 1\ 1\ 1\ ****$

$B_3 = 1\ 1\ 1\ ****$

$B_4 = 1\ 2\ 2\ ****$

$B_5 = 2\ 1\ 2\ ****$

$B_6 = 2\ 2\ 1\ ****$

Case 2 $B_1 = 1\ 1\ 1\ ****$

$B_2 = 1\ 1\ 1\ ****$

$B_3 = 1\ 1\ 2\ ****$

$B_4 = 1\ 2\ 1\ ****$

$B_5 = 2\ 1\ 1\ ****$

$B_6 = 2\ 2\ \gamma\ ****$

where * denotes an elemente of the set $\{\phi\ 1,2\}$ and $\gamma \neq 1$ Suppose that $B_i$'s have the configuration given in Case 1 Each pairset with $x_1 = 1$, $x_2 = x_3 = \phi$ must be contained in exactly one $B_i$ $1 \leq i \leq 4$ without loss of generality let $B_5 = 212\alpha\beta\phi\phi$ and let $P = 1\phi\phi\alpha\phi\phi\phi$ If P is contained in $B_1$ or $B_2$ or $B_3$, say $B^*$ then the pairset $Q = \phi 1\phi\alpha\phi\phi\phi$ will be contained in $B^*$ and $B_5$, a contradiction Otherwise P is contained in $B_4$ and hence the pairset $R = \phi\phi 2\alpha\phi\phi\phi$ is contained in $B_4$ and $B_5$, acontradiction Thus $\beta(5,2,7) > 9$ The proof in Case 2 follows similarly ■

### 3 2 2 Lower bounds for G(k,m,n) from known combinatorial designs

Group covering designs can be used to construct covering designs Such designs are in turn used to further improve the lower bounds for G(k m,n) given by the inequality (3 2) The following results help us in obtaining lower bounds using covering designs and transversal designs

**Theorem 3 2 14** Let m and n be positive integers and let $n \geq m + 1$ Then $C(m+1,1,mn+1) \leq n + G(m+1,m,n)$

**Proof** Let $(Y, \mathcal{G}, \mathcal{P})$ be a minimal group covering design GC[m+1,m,n] and let $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$ Let $y_o \notin Y$ Consider $X = Y \cup \{y_o\}$ and $\mathcal{B} = \mathcal{P} \cup \mathcal{P}'$ where $\mathcal{P}' = \left\{G_1 \cup \{y_o\}, G_2 \cup \{y_o\}, \ldots, G_n \cup \{y_o\}\right\}$ Clearly $|X| = nm + 1$ and

every block of $\mathcal{B}$ has size m + 1 It is easy to verify that $(X\ \mathcal{B})$ is a covering design AD[m+1 1 nm+1] Thus C(m+1 1 nm+1) ≤ n + G(m+1 m n) ■

Let $\Delta(nm+1\ m+1) = C(m+1\ 1\ nm+1) - \alpha(m+1\ 1\ nm+1)$ Using the known bounds for covering numbers we have the following corollary

**Corollary 3 2 15** Let m ≥ (n - 1) Then $G(m+1\ m\ n) \geq \beta(m+1\ m\ n) + \Delta(nm+1\ m+1)$

**Proof** Observe that $\alpha(m+1\ 1\ nm+1) - n = \left\lceil \frac{nm+1}{m+1} \left\lceil \frac{nm}{m} \right\rceil \right\rceil - n = \left\lceil \frac{mn(n-1)}{m+1} \right\rceil = \beta(m+1\ m\ n)$ Thus the result follows from Theorem 3 2 14 ■

**Example** (i) $G(4\ 3\ 6) \geq \beta(4\ 3\ 6) + \Delta(19\ 4)$

$= \beta(4\ 3\ 6) + 2 = 25$

(ii) $G(5\ 4\ 7) \geq \beta(5\ 4\ 7) + \Delta(29\ 5)$

$= \beta(5\ 4,7) + 1 = 35$

**Remark** If n(mn+1) ≡ -1 (mod (m+1)) then by Theorem 2 2 4 we have C(m+1 1 nm+1) ≥ α(m+1 1 nm+1) + 1 and hence G(m+1 m n) ≥ β(m+1 m n) + 1

**Theorem 3 2 16** Let m n and t be positive integers with t ≥ n ≥ 3 If there exists a transversal design TD[n, m] then

$$G(n\ \ m\ \ t(n-1) + 1) \leq tm^2 + G(n\ \ (n-1)m,\ t)$$

**Proof** For each j = 1 2 t let $(X_j, \mathcal{G}_j\ \mathcal{P}_j)$ be a transversal design TD[n m] such that a particular group $G_o$ belongs to all $\mathcal{G}_j$'s and all other groups are pairwise disjoint In other words, $\mathcal{G}_j = \{G_o\ G_{j1}\ \ ,G_{j(n-1)}\}$ where for all j and ℓ 1 ≤ j ≤ t and 1 ≤ ℓ ≤ n-1 $G_o$ and $G_{j\ell}$ are pairwise disjoint groups Let $Y = \bigcup_{j=1}^{t} \bigcup_{\ell=1}^{n-1} G_{j\ell}$, $\mathcal{G} = \left\{ \bigcup_{\ell=1}^{n-1} G_{j\ell} \quad j = 1\ 2 \quad t \right\}$ Then $|Y| = (n-1)mt$ and $|G| = (n-1)m$ for all $G \in \mathcal{G}$ Let $(Y\ \mathcal{G}\ \mathcal{P})$ be the minimal group covering design GC[n m(n-1) t] It is now easy to verify that $(X, \mathcal{H}\ \mathcal{B})$ is a group covering design GC[n m,t(n-1)+1] where $X = Y \cup G_o$, $\mathcal{H} = \{G_{j\ell} \quad 1 \leq$

$J \le t \quad 1 \le \ell \le n-1\} \cup \{G_o\}$ and $\mathcal{B} = \mathcal{P} \cup \mathcal{P}_1 \cup \quad \cup \mathcal{P}_t$ ■

**Corollary 3 2 17** Let m be a prime power such that $m = n - 1 \ge 2$ and let $t \ge n$ If $G(n\ m(n-1)\ t) = \beta(n\ m(n-1)\ t)$ then

$$G(n\ m\ t(n-1)+1) = \beta(n\ m\ t(n-1)+1)$$

**Proof** Note that $\beta(n\ m(n-1)\ t) = \lceil tm^2(n-1)(t-1)/n \rceil$ Since m is a prime power there exists a transversal design TD[n m] by Theorem 3 1 12 Hence by the above theorem

$$G(n\ m\ t(n-1)+1) \le tm^2 + \lceil tm^2(n-1)(t-1)/n \rceil = \beta(n\ m\ t(n-1)+1)$$

Now the result follows from the inequality (3 2) ■

### 3 2 3 Exact bounds for G(k m,n)

In this section the concept of 2-surjectivity (see [13] [31] [40] [64] and [69]) and its connection to special class of group covering designs is studied For each positive integer k ($\ge 2$) an exact bound for the group covering number G(k 2 k) is determined using a result of Kleitman and Spencer [40] The existence of minimum covering designs meeting the Schonheim bound is used to derive an exact bound for a class of group covering designs GC[k k-1 n] Finally constructions are given for few isolated values of k to determine the exact bounds for group covering designs GC[k,2 k+1]

**Definition [31]** An $m \times n$ matrix A over the alphabet $\mathbb{F}_q = \{0\ 1 \quad q-1\}$ is called *2-surjective* if for any two columns $J_1$ and $J_2$ of A and any pair $(x_1\ x_2) \in \mathbb{F}_q^2$, there exists a row i of A such that $A_{i,J_k} = x_k \quad k = 1,2$

Let $S_q(n\ 2)$ denote the minimum number of rows in any 2-surjective matrix with n columns If $n \ge 2$ then

$$S_q(n\ 2) = G(n,q,n) \qquad (3\ 3)$$

If A is an m × n 2-surjective matrix then Kleitman and Spencer [40] have determined the values of $S_2(n,2)$ and have shown that

$$S_2(n\ 2) = \min\left\{ M \;\; n \le \binom{M-1}{\lfloor M/2 \rfloor - 1} \; M \in \mathbb{N} \right\} \tag{3 4}$$

As a consequence of (3 3) and (3 4) we have the following result

**Theorem 3 2 18** If $n(\ge 2)$ is a positive integer then

$$G(n\ 2\ n) = \min\left\{ M \;\; n \le \binom{M-1}{\lfloor M/2 \rfloor - 1} \; M \in \mathbb{N} \right\} \tag{3 5}$$

Many minimum covering designs meet the Schonheim lower bound These covering designs along with Lemma 2 2 7 (with $\lambda = 1$) give exact bounds for G(k m n) for many class of group covering designs

**Theorem 3 2 19** Let $k(\ge 2)$ $n(> k)$ and v be positive integers with $(v - 1) \equiv 0 \pmod{(k-1)}$ $v(v-1)/(k-1) \equiv -2 \pmod{k}$, $n = (v-1)/(k-1)$ and let $v > k(k-2) + 2$ If there exists a minimum covering design AD[k 1 v] with $C(k\ 1\ v) = \alpha(k\ 1\ v)$ then there also exists a minimum group covering design GC[k k-1 n] with $G(k\ k\text{-}1\ n) = \lceil n(n-1)(k-1)/k \rceil$

**Proof** Let $(Y\ \mathcal{P})$ be a covering design AD[k 1 v] with $C(k\ 1,v) = \alpha(k\ 1\ v)$ Then by Lemma 2 2 7 there exists a unique pairset $\{u\ v\} \subseteq Y$ which is contained in exactly k blocks, say $P_i$, $i = 1\ 2, \ldots k$ and all other pairset $\{x,y\} \subseteq Y$ is contained in exactly one block Observe that $P_i \cap P_j = \{u,v\}$ for all $1 \le i < j \le k$ For if $x \in P_i \cap P_j$, $x \notin \{u,v\}$ then $\{x\ u\} \subseteq P_i \cap P_j$, a contradiction to the fact that $\{x\ u\}$ is contained in exactly one block of $\mathcal{P}$ Let $S = \bigcup_{i=1}^{k} P_i$ Clearly $|S| = k(k-2) + 2$ Hence $S \subsetneq Y$ Let $x_0 \in Y\backslash S$ Every pairset containing $x_0$ must be contained in exactly one block of $\mathcal{P}$ Hence there will be exactly $n = (v-1)/(k-1)$ blocks say $T_i$ $1 \le i \le n$ which contains $x_0$ Clearly $\{u,v\} \notin T_i$ for $1 \le i \le n$ Let $X = Y\backslash\{x_0\}$ $\mathcal{S} =$

$\{T_1\backslash\{x_0\} \quad 1 \le i \le n\}$ and let $\mathcal{B} = \mathcal{P}\backslash(T_1 T_2 \quad T_n\}$ Note that for each $B \in \mathcal{B}$ $|T_i \cap B| \le 1$ for $1 \le i \le n$ Since $(Y\ \mathcal{P})$ is a covering design every pairset $\{s\ t\} \subseteq X$ such that s and t are from distinct $T_i\backslash\{x_0\}$ will be contained in a block of $\mathcal{B}$ Hence $(\backslash\ \mathcal{G}\ \mathcal{B})$ is a group covering design $(\ GC[k\ k-1\ n]$ with

$$G(k\ k-1\ n) \le |\mathcal{B}| = \alpha(k\ 1\ v) - (v-1)/(k-1)$$
$$= \lceil n(n(k-1)+1)/k \rceil - n$$
$$= \lceil n(n-1)(k-1)/k \rceil$$

Also from (3 2)

$$G(k\ k-1\ n) \ge \left\lceil \frac{n(k-1)}{k} \left\lceil \frac{(n-1)(k-1)}{k-1} \right\rceil \right\rceil$$
$$= \lceil n(n-1)(k-1)/k \rceil$$

Thus $(\backslash\ \mathcal{G}\ \mathcal{B})$ is a minimum group covering design $GC[k\ k-1\ n]$ with $G(k\ k-1\ n) = \lceil n(n-1)(k-1)/k \rceil$ ■

For $k = 3$ Hanani [28] has shown that a group divisible design $GD[3\ 2\ 2n]$ exists whenever $n \equiv 0 \pmod 3$ and $n \equiv 1 \pmod 3$ and hence

$$G(3\ 2\ n) = \lceil 2n(n-1)/3 \rceil \qquad \text{for } n \equiv 0 \text{ or } 1 \pmod 3$$

If $n = 3t + 2$ for some positive integer t and if $v = 6t + 5$ then Fort and Hedlund [21] have shown that there exists a minimum covering design $AD[3\ 1\ v]$ with $C(3,1,v) = \alpha(k,1\ v)$ On applying Theorem 3 2 19 and Theorem 3 1 12 (for n=3) the following corollary follows immediately

**Corollary 3 2 20** For every positive integer $n \ge 3$

$$G(3\ 2\ n) = \lceil 2n(n-1)/3 \rceil \qquad (3\ 6)$$

For $k = 4$, Brouwer *et al* [11] have shown that a group divisible design $GD[4\ 3,3n]$ exists whenever $n \equiv 0$ or $1 \pmod 4$ and hence

$$G(4,3\ n) = \lceil 3n(n-1)/4 \rceil \qquad \text{for } n \equiv 0 \text{ or } 1 \pmod 4$$

If $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$ and $v = 3n + 1$ then Mills [52], [53]

has shown that there exists a minimum covering design AD[4 1 v] with $C(4\ 1\ v) = \alpha(4\ 1\ v)$ with the exception of $v = 19$ Thus if $v \neq 19$ the conditions of Theorem 3 2 19 are satisfied Hence, we have the following result

**Corollary 3 2 21** For every positive integer $n \geq 4$ $n \neq 6$

$$G(4\ 3\ n) = \lceil 3n(n-1)/4 \rceil \tag{3 7}$$

The case for $n = 4$ follows from Theorem 3 1 12

**Remark** Observe that for $n = 6$ the Corollary 3 2 15 gives $G(4\ 3\ 6) \geq 25 > 23 = \lceil 3n(n-1)/4 \rceil$

For $k = 5$ and $v = 4n + 1$ it has been shown that (see [57]) $C(5\ 1\ v) = \alpha(5\ 1\ v)$ whenever

(i) $n \equiv 2 \pmod 5$ $n > 787$ or

(ii) $n \equiv 4 \pmod 5$ $n > 189$

Thus if $k = 5$ and v satisfies

(i) $v \equiv 9 \pmod{20}$ $v > 3149$ or

(ii) $v \equiv 17 \pmod{20}$, $v > 757$

then the conditions of Theorem 3 2 19 are satisfied Hence we have the following corollary

**Corollary 3 2 22** For every positive integer n satisfying

(i) $n \equiv 2 \pmod 5$, $n > 787$ or

(ii) $n \equiv 4 \pmod 5$ $n > 189$

$$G(5\ 4\ n) = \lceil 4n(n-1)/5 \rceil$$

If $n = k + 1$ and $m = 2$ then by (3 2) and with explicit construction of group covering designs we have the following exact bounds Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design GC[k 2,k+1] and let $\mathcal{G} = \{G_1, \ldots, G_{k+1}\}$ We denote each block $B \in \mathcal{B}$ of size k by $a_i \ldots a_k a_{k+1}$ where $a_i \in G_i \cup \{0\}$, and for each i

$1 \le i \le k+1$ $G_i = \{1\ 2\}$ If $a_i = 0$ for some $i$ then it means that $B \cap G_i = \phi$

**Theorem 3 2 23** (i) $G(3\ 2\ 4) = 8$, (ii) $G(4\ 2\ 5) = 8$

(iii) $G(5\ 2\ 6) = 8$ (iv) $G(6\ 2\ 7) = 7$

**Proof** (i) By (3 2) $G(3\ 2\ 4) \ge 8$ The following eight blocks gives the desired result

| | |
|---|---|
| 1 1 1 0 | 1 0 2 2 |
| 1 2 0 1 | 2 0 1 1 |
| 2 1 0 2 | 0 1 2 1 |
| 2 2 2 0 | 0 2 1 2 |

(ii) By (3 2) $G(4\ 2\ 5) \ge 8$ The following eight blocks gives the desired result

| | |
|---|---|
| 2 1 1 1 0 | 1 1 0 2 2 |
| 1 1 2 0 1 | 1 2 0 1 1 |
| 1 2 1 0 2 | 2 0 1 2 1 |
| 2 2 2 2 0 | 2 0 2 1 2 |

(iii) By (3 2) $G(5\ 2\ 6) \ge 8$ The following eight blocks gives the desired result

| | |
|---|---|
| 1 2 1 1 1 0 | 2 1 1 0 2 2 |
| 1 1 1 2 0 1 | 2 1 2 0 1 1 |
| 1 1 2 1 0 2 | 2 2 0 1 2 1 |
| 1 2 2 2 2 0 | 2 2 0 2 1 2 |

(iv) By (3 2), $G(6,2\ 7) \ge 7$ The following seven blocks gives the desired result

| | |
|---|---|
| 1 2 0 1 2 2 2 | 2 0 1 1 1 2 2 |
| 2 1 1 2 2 2 1 | 0 1 2 1 1 1 1 |
| 2 2 2 0 2 1 2 | 1 2 1 2 1 1 1 |
| 1 1 2 2 2 2 2 | |

■

### 3 2 4 Upper bounds for G(k,m,n)

In this section few constructions for group covering designs are given Group covering designs having bigger group size are constructed from known group covering designs These give tight upper bounds for the group covering number G(k m n) Finally the concept of *labelled covering designs* analogous to that of labelled BIBD given by Zhu [91] is introduced and it is shown that a labelled covering design can be used to construct very good group covering designs Moreover in certain situations these give rise to exact bounds for G(k m n)

Let n k (n > k) be positive integers and let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design GC[k m n] Then for each $B \in \mathcal{B}$ there exists a $G_B \in \mathcal{G}$ such that $G_B \cap B = \phi$ Let $B' = B \cup \{g_B\}$ where $g_B$ is any element in $G_B$ It is easy to verify that $(X\ \mathcal{G}, \mathcal{B}')$ is a group covering design GC[k+1 m n] where $\mathcal{B}' = \{B \quad B \in \mathcal{B}\}$ Thus

$$G(k+1\ m,n) \leq G(k\ m\ n) \tag{3 8}$$

Let n k (n ≥ k) be positive integers and let $(X\ \mathcal{G}\ \mathcal{B})$ be a minimum group covering design GC[k m n+1] Let $\mathcal{G} = \{G_1\ G_2,\ \ G_{n+1}\}$ Delete a group say $G_{n+1}$ from the collection $\mathcal{G}$ If $B \cap G_{n+1} \neq \phi$ for some $B \in \mathcal{B}$ then there exists a group $G_B \in \mathcal{G}$ such that $G_B \cap B = \phi$ Let $g_B \in G_B$ and let $B' = (B \backslash G_{n+1}) \cup \{g_B\}$ for all $B \in \mathcal{B}$ such that $B \cap G_{n+1} \neq \phi$ and $B' = B$ otherwise Let $X' = X \backslash G_{n+1}$ $\mathcal{G}' = \mathcal{G} \backslash \{G_{n+1}\}$ and let $\mathcal{B}' = \{B' \quad B \in \mathcal{B}\}$ It is easy to verify that $(X', \mathcal{G}'\ \mathcal{B}')$ is a group covering design GC[k m n] Thus

$$G(k,m,n) \leq G(k\ m,n+1) \tag{3 9}$$

Let $(X\ \mathcal{G}, \mathcal{B})$ be a group covering design GC[k,m n] and let $\mathcal{G} = \{G_1\ G_2\ \ ,G_n\}$ Let G be a set of m points such that $X \cap G = \phi$ For each $B \in \mathcal{B}$ let $S_B = \{B \cup \{g\} \quad g \in G\}$ Let $\mathcal{B}' = \bigcup_{B \in \mathcal{B}} S_B$, $X' = X \cup G$ and let $\mathcal{G}' =$

$\mathcal{G} \cup \{G\}$ Clearly $(X' \mathcal{G}', \mathcal{B}')$ is a group covering design GC[k+1 m n+1] and $|\mathcal{B}'| = m|\mathcal{B}|$ Thus

$$G(k+1\ m\ n+1) \leq m\ G(k\ m\ n) \tag{3 10}$$

Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design GC[k m n] and let $\mathcal{G} = \{G_1\ G_2\ G_n\}$ Let G be a set of m elements such that $X \cap G = \phi$ Let $X = X \cup G$ and let $\mathcal{G}' = \mathcal{G} \cup \{G\}$ For each $g \in G$ let $\mathcal{B}_g$ be the collection of all distinct k-subsets $B_g$ of X' such that $B_g \cap G = \{g\}$ $|B_g \cap G_i| \leq 1$ for all $1 \leq i \leq n$ and every pairset $\{g\ x\}$ $x \in X$ is contained in some block of $\mathcal{B}_g$ Clearly $|\mathcal{B}_g| = \lceil nm/(k-1) \rceil$ Let $\mathcal{B}' = \mathcal{B} \cup (\bigcup_{g \in G} \mathcal{B}_g)$ Thus $(X'\ \mathcal{G}'\ \mathcal{B}')$ is a group covering design GC[k m n+1] and hence

$$G(k\ m\ n+1) \leq G(k\ m\ n) + m\lceil nm/(k-1) \rceil \tag{3 11}$$

**Theorem 3 2 24** For every positive integer m n k and r with $n \geq k \geq 2$

$$G(k\ mr\ n) \leq G(k\ m,n)\ G(k\ r\ k) \tag{3 12}$$

**Proof** Let $(X\ \mathcal{G}\ \mathcal{B})$ be a group covering design GC[k m n] For each $x \in X$ let $R_x$ denote a set consisting of r elements and for $x\ y \in X$ $R_x \cap R_y = \phi$ On replacing each element $x \in B$ by $R_x$, one can construct a minimum group covering design GC[k r k], $(X_B\ \mathcal{G}_B, \mathcal{P}_B)$ where $X_B = \bigcup_{x \in B} R_x$ and $\mathcal{G}_B = \{R_x\ \ x \in B\}$ For each $G \in \mathcal{G}$, let $G' = \bigcup_{x \in G} R_x$ Let $X' = \bigcup_{x \in X} R_x$, $\mathcal{G}' = \{G'\ \ G \in \mathcal{G}\}$ and $\mathcal{B}' = \bigcup_{B \in \mathcal{B}} \mathcal{P}_B$ Let $\{a\ b\} \subset X'$ such that a and b belong to distinct groups in $\mathcal{G}'$ say $G'_1$ and $G'_2$ respectively Now $a \in R_x$ for some $x \in G_1$ and $b \in R_y$ for some $y \in G_2$ $G_1\ G_2 \in \mathcal{G}$ Then $\{x,y\} \subset X$ is contained in some $B \in \mathcal{B}$ Since $(X_B, \mathcal{G}_B\ \mathcal{P}_B)$ is a group covering design $\{a,b\}$ must be contained in some block of $\mathcal{P}_B$ Thus $(X', \mathcal{G}'\ \mathcal{B}')$ is a group covering design GC[k,mr,n] and

$$G(k,mr,n) \leq G(k,m,n)\ G(k,r,k) \quad \blacksquare$$

**Note** If there exists a group divisible design GD[k,m,n] and a transversal

design TD[k r] we will have equality in (3 12)

For k = 3 and m = 4 Theorem 3 2 24 along with Theorem 3 2 20 gives the following corollary

**Corollary 3 2 25** For every positive integer n

$$\beta(3\ 4\ n) \le G(3,4\ n) \le \beta(3\ 4,n) + 2$$

**Proof**
$$\begin{aligned} G(3\ 4\ n) &\le G(3\ 2\ n)\ G(3\ 2\ 3) \qquad \text{(Theorem 3 2 24)} \\ &= 4G(3\ 2\ n) \\ &= 4\ \lceil 2n(n-1)/3 \rceil \qquad \text{(Theorem 3 2 20)} \end{aligned} \tag{3 13}$$

In [28] Hanani has shown that there exists a GD[3 4 n] for n ≡ 0 or 1 (mod 3) For n ≡ 2 (mod 3) i e n = 3t + 2 for some positive integer t the inequality (3 2) gives

$$G(3\ 4\ 3t+2) \ge \beta(3\ 4\ 3t+2) = 8t(3t+1) + 16t + 6$$

Whereas 3 13 gives

$$\begin{aligned} G(3\ 4,3t+2) &\le 4\ \lceil 2(3t+1)(3t+2)/3 \rceil \\ &= 8t(3t+1) + 16t + 8 \quad \blacksquare \end{aligned}$$

If n = k in a group covering design then we have the following trivial result

**Theorem 3 2 26** Let m and k be positive integers, k ≥ 2 Then

$$G(k\ m,k) \le G(k+1\ m\ k+1)$$

**Proof** The restriction of the elements of blocks of a group covering design GC[k+1 m k+1] to the first k groups gives the desired result ■

Suppose that (X,G,$\mathcal{B}$) is a group covering design GC[k,m,n] Let $\mathcal{G}$ = $\{G_1, G_2, \ldots, G_n\}$ Define a mapping f $X \longrightarrow Y = \{y_1, y_2, \ldots y_n\}$ such that f(x) = $y_i$ iff $x \in G_i$ Let f(B) = {f(x) x ∈ B} and f($\mathcal{B}$) = {f(B) B ∈ $\mathcal{B}$} then clearly (Y f($\mathcal{B}$)) is a covering design AD[k $m^2$,n] and

$$C(k,m^2,n) \le G(k\ m\ n)$$

It is also possible to construct a group covering design from a labelled covering design a covering design whose blocks are labelled in a particular fashion Below we define a labelled covering design following the definition of labelled BIBD [91]

Definition Let $(Y\ \mathcal{B})$ be a covering design AD[k m n] and let G be an additive group of order m say $\mathbb{Z}_m$ $(Y\ \mathcal{B})$ will be called a *labelled covering design* $AD^*[k\ m\ n]$ if for each $B \in \mathcal{B}$ there exists $f_B$ $B \longrightarrow G$ such that for every pairset $\{x\ y\} \subseteq Y$

$$\left\{ f_{B_i}(x) - f_{B_j}(y) \quad B_j \in \mathcal{B} \text{ and contains the pairset } \{x\ y\} \right\} = G$$

We relabel the block $B \in \mathcal{B}$ by $B^* = \{(x\ f_B(x)) \quad x \in B\}$

Example The following blocks on the set $X = \{0\ 1\ 2\ x\ y\}$ gives an AD[3 2 5]

$\{0\ 1,x\}$ $\{0\ 1\ y\}$ $\{2\ 0\ x\}$ $\{2\ 0\ y\}$

$\{1\ 2\ x\}$ $\{1,2\ y\}$ $\{0\ x\ y\}$ $\{0\ x\ y\}$

Note the following relabelling of the blocks gives a labelled covering design $AD^*[3\ 2\ 5]$ Let $G = \{0,1\}$ The blocks of labelled covering design are

$\{(0\ 0)\ (1\ 0),\ (x\ 1)\}$, $\{(0,0)\ (1\ 1)\ (y\ 0)\}$,

$\{(2\ 0)\ (0\ 0)\ (x,1)\}$ $\{(2,1)\ (0\ 0),\ (y\ 1)\}$

$\{(1\ 0)\ (2,0),\ (x,0)\}$, $\{(1,0)\ (2,1)\ (y,0)\}$

$\{(0\ 0)\ (x,0),\ (y,0)\}$, $\{(0,0),\ (x\ 0),\ (y\ 1)\}$

Theorem 3 2 27 If there exists a labelled covering design $AD^*[k\ m\ n]$ then there exists a group covering design GC[k m n] with $G(k,m\ n) = mC(k\ m,n)$

Proof Let $(Y,\mathcal{B})$ be a labelled covering design $AD^*[k,m,n]$ and let G be an additive group of order m, say $\mathbb{Z}_m$ Then for each $B \in \mathcal{B}$ there exists a function $f_B$ $B \longrightarrow G$ such that for every pairset $\{x\ y\} \subseteq Y$, $\left\{ f_{B_i}(x) - f_{B_j}(y) \right.$

$B_1 \in \mathcal{B}$ and contains $(x\ y)\Big\} = G$ For each $y \in Y$ let $G_y = \langle y \rangle \times G$

Let $X = Y \times G$ $\mathcal{G} = \{G_y \quad y \in Y\}$ $G(B^*) = \left\{\langle (x\ f_B(x)+g) \quad x \in B\rangle \quad g \in G\right\}$

and $\mathcal{A} = \bigcup_{B \in \mathcal{B}} G(B^*)$ Let $\langle (y_1, \imath), (y_2, \jmath)\rangle \subseteq X$ be any pairset Then there will be a block $B^*$ containing the pairset $\langle (y_1, \imath') \quad (y_2, \jmath')\rangle$ such that $f_B(y_1) - f_B(y_2) = \imath' - \jmath' = \imath - \jmath \in \mathbb{Z}_m$ Hence by construction $G(B^*)$ will have a block containing the pairset $\langle (y_1, \imath), (y_2, \jmath)\rangle$ Thus $(X\ \mathcal{G}\ \mathcal{A})$ is a group covering design $GC[k\ m\ n]$ with $G(k\ m\ n) = mC(k\ m\ n)$ ■

Though many researchers (see [4] [28]) have given constructions for covering design of small block size and of index $m > 1$ it is not always true that they will also be labelled covering design But the existence of a labelled covering design meeting the Schonheim lower bound ensures the equality in (3 2) in certain situation as shown by the following theorem

**Theorem 3 2 28** Suppose $AD[k\ m\ n]$ be a covering design which is also a labelled covering design such that $C(k,m\ n) = \alpha(k\ m\ n)$ If $n\lceil m(n-1)/(k-1)\rceil \equiv \ell \pmod k$ and if $\ell > k(m-1)/m$ then

$$G(k\ m\ n) = \left\lceil \frac{mn}{k} \left\lceil \frac{m(n-1)}{k-1} \right\rceil \right\rceil \equiv \beta(k\ m\ n)$$

**Proof** From the previous theorem

$$G(k\ m\ n) \leq m\ C(k,m,n) = m \left\lceil \frac{n}{k} \left\lceil \frac{(n-1)m}{k-1} \right\rceil \right\rceil$$

$$= m \left( \frac{nP_0 - \ell}{k} + 1 \right)$$

where $P_0 = \lceil m(n-1)/(k-1) \rceil$ Also from (3 2)

$$G(k\ m,n) \geq \left\lceil \frac{nm}{k} \left\lceil \frac{m(n-1)}{k-1} \right\rceil \right\rceil = \left\lceil \frac{nm\ P_0}{k} \right\rceil$$

$$= \left\lceil \frac{m(nP_0 - \ell)}{k} + \frac{m\ell}{k} \right\rceil$$

$$= m \left( \frac{nP_o - \ell}{k} + 1 \right)$$

Hence the result follows ■

Note In the above theorem if $\ell = 0$ then the result follows immediately

Using the results proved so far we construct the following tables (Table 3.1 - 3.3)

Table 3.1 Lower Bounds on $G(k,2,n)$

| $n$ \ $k$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 | [7]4 | | | | | | | | | |
| 4 | [7]8 | [7]5 | | | | | | | | |
| 5 | [7]11 | [w]8 | [7]6 | | | | | | | |
| 6 | [7]20 | 12 | [w]8 | [7]6 | | | | | | |
| 7 | [7]28 | [v]14 | [7]10 | [w]7* | [7]6 | | | | | |
| 8 | [7]38 | 20 | 13 | 8 | 7 | [7]6* | | | | |
| 9 | [7]48 | 27 | 15 | 12 | 8 | 7 | [7]6* | | | |
| 10 | [7]60 | [v]30 | 20 | 14 | [f]10 | 8 | 7 | [7]6* | | |
| 11 | [7]74 | 39 | 22 | [c]16 | 13 | 9 | 8 | 7 | [7]7 | |
| 12 | [7]88 | 48 | 29 | 20 | 14 | 12 | 8 | 8 | 7 | [7]7* |
| 13 | [7]104 | [7]52 | 32 | 22 | [d]16 | 13 | [f]10 | 8 | 8 | 7 |
| 14 | 122 | 63 | 40 | 28 | 20 | 14 | 13 | 9 | 8 | 7 |
| 15 | [7]140 | 75 | 42 | 30 | 22 | [a]16 | 14 | 12 | 9 | 8 |
| 16 | [7]160 | [v]80 | 52 | 32 | [d]21 | 20 | 15 | 13 | [f]10 | 8 |
| 17 | [7]182 | 91 | 55 | 40 | 30 | 22 | 16 | 14 | 13 | 9 |
| 18 | [7]204 | 108 | 65 | 42 | 31 | 23 | 20 | 15 | 14 | 12 |
| 19 | [7]228 | [v]111 | 69 | [o]1 | 33 | 29 | 22 | 16 | 14 | 13 |
| 20 | [7]254 | 130 | 80 | [o]4 | 40 | 30 | 23 | 20 | 15 | 14 |

Table 3.2 Lower Bounds on $G(k,3,n)$

| $n$ \ $k$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 | [v]9 | | | | | | | | | |
| 4 | 20 | [b]9 | | | | | | | | |
| 5 | [v]30 | [f]15* | [z]11 | | | | | | | |
| 6 | 18 | [h]25 | 15 | [z]11 | | | | | | |
| 7 | [v]63 | [f]32 | 21 | 14 | [z]11 | | | | | |
| 8 | 88 | [f]42* | 29 | 20 | 14 | [z]11 | | | | |
| 9 | [v]108 | [f]54* | 33 | 23 | 16 | 14 | [z]11 | | | |
| 10 | 140 | [f]68 | 42 | 30 | 22 | 15 | 14 | [z]11 | | |
| 11 | [v]165* | [f]83* | 53 | 33 | 24 | 21 | 15 | 14 | [z]11 | |
| 12 | 204 | [f]99 | 65 | 42 | 31 | 23 | 20 | 15 | 14 | [z]11 |
| 13 | [v]234 | [f]117 | 71 | 52 | 34 | 30 | 22 | 16 | 15 | 13 |
| 14 | 280 | [f]137 | 84 | [o]6 | 42 | 32 | 24 | 21 | 16 | 14 |
| 15 | [v]315* | [f]158* | 99 | 68 | 45 | [e]35 | 30 | 23 | 21 | 15 |
| 16 | 368 | [f]180 | 116 | 72 | 55 | 42 | 32 | [a]25 | 22 | 20 |
| 17 | [v]408 | [f]204* | 123 | 85 | 59 | 45 | [a]35 | 31 | 24 | 22 |
| 18 | 168 | [f]230* | 141 | 99 | 70 | 54 | 42 | 33 | 30 | 23 |
| 19 | [v]513* | [f]257* | 160 | 105 | 74 | 57 | 45 | 35 | 32 | 24 |
| 20 | 580 | [f]285 | 180 | 120 | 86 | 68 | 54 | 42 | 33 | 30 |

Table 3.3: Lower Bounds on $G(k,4,n)$

| $n$ \ $k$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 | [b]16 | | | | | | | | | |
| 4 | [w]42 | [w]16 | | | | | | | | |
| 5 | 54 | 30 | [b]16 | | | | | | | |
| 6 | [w]80 | 42 | 21 | [c]17 | | | | | | |
| 7 | [w]112 | [w]56* | [c]35 | 24 | [c]17 | | | | | |
| 8 | 150 | 80 | [d]16 | 32 | 23 | [c]17 | | | | |
| 9 | [w]192 | 99 | 58 | 42 | 31 | 23 | [c]17 | | | |
| 10 | [w]240 | [w]120* | 72 | 51 | 35 | 30 | 23 | [c]17 | | |
| 11 | 304 | 154 | 88 | 59 | 41 | 33 | 25 | 22 | [c]17 | |
| 12 | [w]352 | 180 | 106 | 72 | 55 | 42 | 32 | 24 | 22 | [c]17 |
| 13 | [w]416 | [w]208 | [d]126 | 87 | 60 | 46 | [f]36 | 32 | 24 | 22 |
| 14 | 486 | 242 | 146 | 103 | 72 | 56 | 41 | 34 | 31 | 24 |
| 15 | [w]560* | 285 | 168 | 120 | 86 | 60 | 47 | 42 | 33 | 30 |
| 16 | [w]640 | [w]320* | 192 | 128 | 92 | 72 | 57 | 45 | [d]36 | 32 |
| 17 | [c]736 | 371 | 218 | 148 | 107 | 85 | 61 | 55 | 44 | 34 |
| 18 | [w]816 | 414 | [f]216 | 168 | 124 | 90 | 72 | 58 | 46 | 42 |
| 19 | [w]912* | [w]456 | 271 | 190 | 131 | 105 | 76 | [e]62 | 56 | 45 |
| 20 | 1014 | 520 | 301 | 211 | 149 | 110 | 89 | 72 | 59 | 47 |

## Key to Tables 3.1-3.3

| | | | |
|---|---|---|---|
| * | Exact bound | $h$ | Corollary 3.2.15 |
| Unmarked | Theorem 3.2.1 | $i$ | Theorem 3.2.18 |
| | Corollary 3.1.4 and Theorem 3.2.2 | $j$ | Corollary 3.2.20 |
| $b$ | Theorem 3.1.12 | $l$ | Corollary 3.2.21 |
| | Theorem 3.2.3 | $w$ | Corollary 3.2.23 |
| $c$ | Corollary 3.2.6 | $x$ | Theorem 3.2.26 |
| $e$ | Corollary 3.2.9 | $y$ | Hanani [28] |
| $f$ | Corollary 3.2.12 | $z$ | Sloane [69] |
| $g$ | Theorem 3.2.13 | | |

# CHAPTER IV

## LOWER BOUNDS ON BINARY COVERING CODES

In this chapter, we use a simple observation of Zhang's result [88] to generalise Honkala's idea as discussed in [31]. This leads to nineteen improvements in the existing lower bounds [14, Table 6.1] of K(n,R).

Let C be an (n,M)R code. The sphere covering bound (2.6) gives

$$|C| \geq 2^n/V(n,R). \tag{4.1}$$

Many ad hoc methods are used to improve the sphere covering bound [16],[30]. However, the most significant improvements to the sphere covering bound are due to van Wee [80]. It has recently been discovered that an early paper by Johnson [35] contains, e.g., the main approaches described in [80] and [88] (see [14], pp. 177-178). van Wee gave an estimation of the excess on the spheres of radius two centered at the points which have distance R-1 or R to the code. In particular, he has proved the following result.

**Lemma 4.1** [80, Lemma 9]: Let $n,R \in \mathbb{N}$, $n \geq 2R$, $\mathbf{x} \in \mathbb{F}_2^n$ and let C be an (n,M)R code. If $d(\mathbf{x},C) \geq R-1$ then

$$E_C(B_2(\mathbf{x})) \geq \varepsilon_0 = \binom{R+2}{2}\left\lceil \frac{\binom{n-R+1}{2}}{\binom{R+2}{2}} \right\rceil - \binom{n-R+1}{2} \tag{4.2}$$



Using the above lemma and a suitable averaging method,he proved that (Theorem 2.1.2) for all $n,R \in \mathbb{N}$ with $n \geq 2R$,

$$K(n,R) \geq \frac{(V(n,2) - \mu + \varepsilon_0)2^n}{(V(n,2)-\mu)\,V(n,R) + \varepsilon_0 V(n,R-2)} \tag{4.3}$$

where $\varepsilon_0$ is as in (4.2) and $\mu = (R+2)(R-1)/2$.

In [31], Honkala modified van Wee's bound on K(n,R) as in (4.3) by

giving a better estimation than (4.2) for spheres of radius two with center at the points which are at a distance R-1 or R to the code C and are covered by *exactly* one codeword (Lemma 2.1.3). In [88], Zhang has proved the following inequality which is useful in proving the main theorem of this chapter.

**Lemma 4.2** [88, Lemma 4]: For any code with covering radius R, we have

$$\min\Big\{A_{R+1}(\mathbf{x}) + A_{R+2}(\mathbf{x}) : A_o(\mathbf{x}) = \ldots = A_{R-2}(\mathbf{x}) = 0,\ A_{R-1}(\mathbf{x}) + A_R(\mathbf{x}) = k\Big\} \geq C(R+2,1;n-kR+1),$$

where C(k,1;v) is the minimal number of k-subsets of a given v-set needed to cover all the unordered pairs of the same v-set and

$$A_i(\mathbf{x}) = |\{c \in C : d(\mathbf{x}, \mathbf{c}) = i\}|.$$

The notations f(v,k) and C(v,k,2) are used in [31] and [88],respectively,instead of C(k,1;v). In other words, for any $\mathbf{x}$ with $\mathbf{x} \in A \cap Z_{k-1}(C)$, we have

$$|B_{R+2}(\mathbf{x}) \cap C| \geq k + C(R+2,1;n-kR+1) \tag{4.4}$$

where

$$Z_i(C) = \{\mathbf{x} \in \mathbb{F}_2^n : |B_R(\mathbf{x}) \cap C| = i + 1\}$$

and

$$A = \{\mathbf{x} \in \mathbb{F}_2^n : d(\mathbf{x},C) \geq R-1\}.$$

For the sake of convenience, we repeat the following notations for q = 2 as discussed in Chapter II .

$$Z(C) = \{\mathbf{x} \in \mathbf{F}_2^n : |B_R(\mathbf{x}) \cap C| > 1\},$$

$$E_C(\mathbb{F}_2^n) = |C|V(n,R) - 2^n, \tag{4.5}$$

$$E_C(V) = \sum_i i|Z_i(C) \cap V| \tag{4.6}$$

**Proof** Without loss of generality we assume $\mathbf{x} = \phi$ the element of $\mathbb{F}_2^n$ of weight zero and consider the following two cases

**Case I** $A_{R-1}(\phi) \neq 0$ Then all vectors of weight one in $B_2(\phi)$ are covered Since $\phi \in Z_1 \cap Y_J$, there will be exactly $(J+1)$ codewords $c_1, c_2, \ldots, c_{J+1}$ such that for $1 \leq \ell, k \leq J+1$ $wt(c_\ell) \in \{R-1, R\}$ $1 \leq d(c_\ell, c_k) \leq 2J$ with $\ell \neq k$ and there is at least one pair say $c_1$ and $c_2$ such that $d(c_1, c_2) = 2J$ or $2J-1$ Now for each $\ell$ $1 \leq \ell \leq J+1$ let $s_\ell = \{j \mid c_\ell(j) = 1\}$ and $S = \bigcup_{\ell=1}^{J+1} s_\ell$ The uncovered elements of weight two in $B_2(\phi)$ are all the 2-subsets of $S$ the complement of $S$ These elements must be covered by the codewords of weight $(R+1)$ or $(R+2)$ Clearly it is better to use only codewords of weight $(R+2)$ to cover the weight two vectors of $B_2(\phi)$ Since the largest pairwise distance in $(B_R(\phi) \cap C)$ is $2J$ or $(2J-1)$ we have $|S^c| \geq n - (R-1) - 1J$ Hence by Lemma 4.2, $A_{R+1}(\phi) + A_{R+2}(\phi) \geq C(R+2, 1, n-R+1-1J)$

**Case II** Suppose $A_{R-1}(\phi) = 0$ Hence all the vectors in $B_2(\phi)$ are covered by the codewords having weight at least $R$ Let $s_\ell$ be as defined in Case I above Here $|s_\ell| = R$ for $\ell = 1, 2, \ldots, J+1$ Hence $|S^c| \geq n - R - 1J$ The 1-subsets and 2-subsets of $S^c$ are the vectors in $B_2(\phi)$ which remain uncovered They have to be covered by the codewords of weight $(R+1)$ or $(R+2)$ The problem of covering all 1- and 2-subsets of a given set of cardinality $(n-R-1J)$ by $(R+1)$- and $(R+2)$-subsets of the given set with covering radius $R$, is equivalent to the problem of covering all of the 2-subsets of a set of cardinality $(n-R+1-1J)$ by only $(R+2)$-subsets Thus $A_{R+1}(\phi) + A_{R+2}(\phi) \geq C(R+2, 1, n-R+1-1J)$ ■

**Corollary 4.6** If $1 < n-R+1-1J \leq R+2$, then $A_{R+1}(x) + A_{R+1}(x) \geq 1$ for any $x \in Y_J \cap Z_1$

**Proof** Since $n-R+1-1J \geq 2$ at least one vector of weight two having (nonzero coordinates in $S^c$ remains to be covered by a codeword of weight

(R+1) or (R+2) Hence $A_{R+1}(x) + A_{R+2}(x) \geq 1$ ■

**Lemma 4 7** For every $x \in Y_j \cap Z_l$ $E_C(B_2(x)) \geq \varepsilon_{lj}$ where

$$\varepsilon_{lj} = (l+1)[1 + (n-R+1)R + \binom{R}{2}] + \binom{R+2}{2}C(R+2,1\ n-R+1-l_j) - V(n,2)$$

**Proof** Let $c \in C$ If $d(x\ c) \in \{R-1\ R\}$ then

$$|B_2(x) \cap B_R(c)| = 1 + (n - R + 1)R + \binom{R}{2}$$

If $d(x\ c) \in \{R-1\ R+2\}$ then $|B_2(x) \cap B_R(c)| = \binom{R+2}{2}$

If $d(x\ c)$ $R + 2$ then $|B_2(x) \cap B_R(c)| = 0$

Now the result follows from (2 8) and Lemma 4 5 notably

$$E_C(B(x)) = \sum_{c \in C} |B_R(c) \cap B_2(x)| - |B_2(x)|$$

$$= \left( A_{R-1}(x) + A_R(x)\right)\left( 1 + (n-R+1) + \left( \begin{matrix} R \\ 2 \end{matrix} \right)\right)$$

$$+\left(A_{R+1}(x) + A_{R+2}(x)\right)\binom{R+2}{2} - V(n\ 2)$$

$$\geq (l+1)\left(1 + (n-R+1)R + \binom{R}{2}\right)$$

$$+ \binom{R+2}{2}C(R+2,1\ n-R+1-l_j) - V(n,2) \quad ■$$

**Theorem 4 8** Let $n \geq 2R + 1$ Then

$$K(n\ R) \geq \frac{(V(n,2) - \mu + \varepsilon)2^n}{(V(n,2) - \mu)V(n,R) + \varepsilon V(n\ R-2)},$$

where $\varepsilon = C(R+2,1\ n-R+1)\binom{R+2}{2} - \binom{n-R+1}{2}$

$$\mu_1 = 2 + n(R-2) - \binom{R-2}{2}, \qquad \mu_2 = \min_{\substack{l \geq 1 \\ 1 \leq j \leq R}} \left\{ \Delta_j + \frac{\varepsilon_{lj} - \varepsilon}{l} \right\}$$

and $$\mu = \begin{cases} \mu_2 & \text{if } R = 1 \\ \min(\mu_1,\mu_2), & \text{if } R \geq 2 \end{cases}$$

where $\Delta_j$ and $\varepsilon_{lj}$ are as in Lemma 4 3 and Lemma 4 7 respectively

**Proof** Substituting the bounds for excess $E_C(B_2(x))$ obtained by Lemmas 4 4 and 4 7 in (2 8) we get

$$\sum_{x\in A} E_C(B_2(x)) = \sum_{x\in A\setminus Z} E_C(B_2(x)) + \sum_{x\in A\cap Z} E_C(B_2(x))$$

$$= \sum_{x\in A\setminus Z} E_C(B_2(x)) + \sum_{j=1}^{R} \sum_{i>0} \sum_{x\in Y_j\cap Z_i} E_C(B_2(x))$$

$$\geq \varepsilon(|A| - \sum_{j=1}^{R} \sum_{i>0} |Y_j \cap Z_i|) + \sum_{j=1}^{R} \sum_{i>0} \varepsilon_{ij}|Y_j \cap Z_i| \qquad (4\,8)$$

In [31] Honkala has shown that for $z \in Y$

$$|A \cap B_2(z)| \leq V(n,2) - \mu_1 \quad \text{where } \mu_1 = 2 + n(R-2) - \binom{R-2}{2} \qquad (4\,9)$$

Using Lemma 4 3 (4 6) (4 7) and (4 9) we have

$$\sum_{x\in A} E_C(B_2(x)) = \sum_{x\in A} \sum_{i>0} i|Z_i \cap B_2(x)|$$

$$= \sum_{i} i \sum_{z\in Z_i} |A \cap B_2(z)|$$

$$\leq \sum_{i} i \sum_{z\in Y\cap Z_i} (V(n,2) - \mu_1) + \sum_{j=1}^{R} \sum_{i>0} i \sum_{z\in Y_j\cap Z_i} (V(n,2) - \Delta_j)$$

Combining this with (4 8) gives

$$\varepsilon(|A|) \leq \sum_{i} i|Y \cap Z_i|(V(n,2) - \mu_1)$$

$$+ \sum_{j=1}^{R} \sum_{i>} i|Y_j \cap Z_i|(V(n,2) - \Delta_j - \frac{\varepsilon_{ij}}{i} + \frac{\varepsilon}{i})$$

i e $$\varepsilon(|A|) \leq (V(n,2) - \mu) \sum_{i} i|Y \cap Z_i|$$

$$+ (V(n,2) - \mu) \sum_{j=1}^{R} \sum_{i} i|Y_j \cap Z_i|$$

where $\mu$ is as defined in the theorem Hence

$$\varepsilon|A| \leq (V(n,2) - \mu)(\sum_{i>0} i|Z_i|)$$

since $|A| \geq 2^n - |C|V(n,R-2)$ we have

$$\varepsilon( 2^n - |C|V(n,R-2) ) \leq (V(n,2) - \mu)(|C|V(n,R) - 2^n)$$

from which the result follows ■

Example 4.1 $K(24,3) \geq 8128$

In this case $\mu_1 = 26$ $\Delta_j = 3 + j(3-j) + \binom{j}{2}$, $\varepsilon = 39$ $\mu_2 = -4$ and hence $\mu = -4$ Using these quantities in Theorem 4.8, we have

$$K(24,3) \geq 8128$$

whereas 8123 is listed in [14 Table 6.1]

Remark In [79], van Wee has conjectured that $K(24,3) = 8192$ Observe that the sphere covering bound gives $K(24,3) \geq 7217$ only

Example 4.2 $K(19,3) \geq 513$

In this case $\mu_1 = 21$, $\Delta_j = 3 + j(3-j) + \binom{j}{2}$, $\varepsilon = 24$ $\mu_2 = 16$ and hence $\mu = 16$ Using these quantities in Theorem 4.8, we have

$$K(19,3) \geq 513$$

where 511 is listed in [14 Table 6.1]

The above example provides a simple proof of the following corollary that has already been proved in [14]

Corollary 4.9 $t[19,9] = 4$

Proof From Example 4.2, $K(19,3) \geq 513 > 2^9$ i.e. the binary code [19,9]3 does not exist Since $3 \leq t[19,9] \leq 4$ (see Table 1 [22]) we have $t[19,9] = 4$ ■

When applied to particular values of n and R, Theorem 4.8 gives the following nineteen improvements The values of C(k,1,v) are from Table 2.1

Corollary 4.10

| | |
|---|---|
| K(27,2) ≥ 380463 (380328) | K(19,3) ≥ 513 (511) |
| K(24,3) ≥ 8128 (8123) | K(26,3) ≥ 24235 (24210) |
| K(25,3) ≥ 80835 (80720) | K(33,3) ≥ 1516208 (1516050) |
| K(14,4) ≥ 16 (15) | K(23,4) ≥ 909 (903) |
| K(26,4) ≥ 4270 (4263) | K(28,4) ≥ 12410 (12370) |
| K(33,4) ≥ 193273(193045) | K(28,5) ≥ 2641 (2629) |
| K(20,6) ≥ 24 (23) | K(26,6) ≥ 275 (272) |
| K(30,7) ≥ 486 (483) | K(26,8) ≥ 36 (35) |
| K(32,8) ≥ 369 (366) | K(29,9) ≥ 43 (42) |
| K(32,10) ≥ 53 (51) | |

The numbers within parentheses are the known lower bounds for K(n,R) (see Table 6.1 [14].)

# CHAPTER V

## LOWER BOUNDS FOR q-ARY COVERING CODES

In the preceding chapter we have discussed the lower bounds for $K(n, R)$ and have obtained nineteen improvements in the existing lower bounds for $K(n, R)$ [14 Table 6.1]. In the present chapter we extend the techniques used in Chapter IV to the case $q > 2$, $q \in \mathbb{N}$ by relating group covering designs to q-ary covering codes. This in addition to some other counting arguments gives a better estimation for the excess than those of Lemma 2.1.5 for many pair of values of n and R. It leads to improvements in the existing lower bounds for $K_q(n, R)$ in some cases.

Throughout this chapter, we assume that C is a $(q, n, M)R$ code, $q \geq 3$. Also recall that the alphabet $\mathbb{F}_q$ is the set $\{0, 1, \ldots, q-1\}$. Let $(X, \mathcal{G}, \mathcal{B})$ be a group covering design $GC[k, m, n]$ where X is a finite set of mn elements, $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$ is a partition of X where each part $G_i$ (called *groups*) is of size m and $\mathcal{B}$ is a collection of k-subsets (called *blocks*) of X such that every unordered pair from distinct groups of $\mathcal{G}$ is contained in at least one element of $\mathcal{B}$ and $|B_i \cap G_j| \leq 1$ for every $B_i \in \mathcal{B}$ and $G_j \in \mathcal{G}$. The group covering number $G(k, m, n)$ is defined as

$$G(k, m, n) = \min \{|\mathcal{B}| : (X, \mathcal{G}, \mathcal{B}) \text{ is a } GC[k, m, n]\}$$

We now use the quantity $G(k, m, n)$ to derive a linear inequality for C. For $\mathbf{x} \in \mathbb{F}_q^n$, let

$$A_i(\mathbf{x}) = |\{ c \in C : d(\mathbf{x}, c) = i \}|$$

For $\mathbf{x} = \phi$, the element of $\mathbb{F}_q^n$ of weight 0, we will simply write $A_R$ instead of $A_R(\phi)$. Throughout this chapter, we denote

$$A = \{ x \in \mathbb{F}_q^n \quad d(x\,C) \geq R - 1 \}$$

and $Z$ is as in (2.10) i.e.

$$Z = \{ x \in \mathbb{F}_q^n \quad |B_R(x) \cap C| > 1 \}$$

We say that an element $x \in \mathbb{F}_q^n$ is covered by a word $s \in \mathbb{F}_q^n$ or by set $S \subseteq \mathbb{F}_q^n$ if $d(x\,s) \leq R$ or $d(x\,S) = \min_{s \in S} d(x\,s) \leq R$ respectively. The set of points covered by $S$ is denoted by $B_R(S)$. In the following lemmas we analyze how the sphere $B_2(x)$ of radius two is covered by the spheres $B_R(C)$.

Lemma 5.1. Let $x \in \mathbb{F}_q^n$. Then for any code with covering radius $R$ and $n \geq 2R+1$ we have

$$\min\Big\{A_{R-2}(x),\ A_0(x) = \cdots = A_{R-2}(x) = A_R(x) = \cdots = A_{R+1}(x) = 0,\ A_{R-1}(x) = 1\Big\} \geq G(R+2,\ q-1,\ n-R+1)$$

Proof. Without loss of generality (w.l.o.g.) $x = \phi$ (we can always use a suitable translation). Asssume that w.l.o.g. $c$ is a codeword of weight $R-1$ satisfying $c(R) = \cdots = c(n) = 0$. All the elements of weight one in $B_2(\phi)$ are covered by the codeword $c$. Any element $y \in \mathbb{F}_q^n$ of weight two in $B_2(\phi)$ is covered by $c$ if $y(i) \neq 0$ for some $i$, $1 \leq i \leq R-1$. For any $x \in \mathbb{F}_q^n$ let the set $S = \{(i,\alpha),\ 1 \leq i \leq n,\ \alpha \in \mathbb{F}_q \setminus \{0\} \quad x(i) = \alpha\}$ represent the element $x$. Then the uncovered elements of weight two are all pairsets $\{(i\ \alpha)\ (j\ \beta)\}$ $i \neq j$, of the set $X = \{(i,\alpha) \quad \alpha \in \mathbb{F}_q \setminus \{0\},\ R \leq i \leq n\}$. Those elements must be covered by codewords of weight $R+2$. Let $\mathcal{G} = \{G_R, G_{R+1}, \ldots, G_n\}$ where for every $j$, $R \leq j \leq n$, $G_j = \{(j,\alpha) \quad \alpha \in \mathbb{F}_q \setminus \{0\}\}$. Clearly $\mathcal{G}$ is a partition of $X$, $|\mathcal{G}| = n - R + 1$ and each $G_j \in \mathcal{G}$ is of size $(q-1)$. From the definition of $G(k,m,n)$ we must have

$$A_{R+2} \geq G(R+2,\ q-1,\ n-R+1) \quad \blacksquare$$

Lemma 5 2 Let $R+2 \le n \le 2R$ Then, for any code with covering radius $R > 1$ and for any $x \in \mathbb{F}_q^n$ we have

$$\min\Big\{A_{R-2}(x),\ A_0(x) = \cdots = A_{R-2}(x) = A_R(x) = A_{R-1}(x) = 0,\ A_{R-1}(x) = 1\Big\} \ge G(n-R+1,\ q-1,\ n-R+1)$$

Proof W l o g we assume that $x = \phi$ Let c be the codeword of weight R-1 satisfying $c(R) = \cdots = c(n) = 0$ For any $x \in \mathbb{F}_q^n$ let the set $S = \{(i\ \alpha)\ \alpha \in \mathbb{F}_q \setminus \{0\}\ \ 1 \le i \le n\ \ x(i) = \alpha\}$ represent the element x Hence the uncovered elements in $B_2(\phi)$ are all 2-subsets $\{(i\ \alpha)\ (j\ \beta)\}$, $i \ne j$ of the set $X = \{(i\ \alpha)\ \ \alpha \in \mathbb{F}_q \setminus \{0\}\ \ R \le i \le n\}$ Those must be covered by codewords of weight R + ? Since n - R + 1 < R + 2 it is always better to use only codewords c' of weight R + ? with $c'(i) \ne 0$ for all i $R \le i \le n$ and let $\mathcal{A} = \{c_1, c_2, \ldots, c_\ell\}$ be such a collection of codewords Let $\mathcal{G} = \{G_R, \ldots, G_n\}$ be a partition of X where for each j $R \le j \le n$ $G_j = \{(j\ \alpha)\ \ \alpha \in \mathbb{F}_q \setminus \{0\}\}$ For each $a \in \mathcal{A}$ let $B_a \subseteq X$ be such that for $j \in \{R, \ldots, n\}$ $(j\ a(j)) \in B_a \cap G_j$ Clearly $|B_a| = n-R+1$ Let $\mathcal{B} = \{B_a\ \ a \in \mathcal{A}\}$ It is easy to verify that $(X, \mathcal{G}, \mathcal{B})$ is a group covering design GC[n-R+1,q-1 n-R+1] From the definition of G(k,m n), we must have

$$|\mathcal{A}| = \ell \ge G(n-R+1,\ q-1,\ n-R+1)$$

Thus the result follows ∎

Lemma 5 3 Let $x \in \mathbb{F}_q^n$ Then for any code with covering radius R and $n \ge 2R+1$, we have

$$\min\Big\{A_{R+1}(x),\ A_0(x) = \cdots = A_{R-2}(x) = A_R(x) = \cdots = A_{R-2}(x) = 0,\ A_{R-1}(x) = 1\Big\} \ge \left\lceil \frac{n-R+1}{R+1} \left\lceil \frac{(n-R)(q-1)}{R} \right\rceil \right\rceil \equiv \alpha_0 \text{ (say)} \qquad (5\ 1)$$

Proof W l o g let $x = \phi$ Let $c \in C$ be the codeword of weight R - 1 satisfying $c(R) = \quad = c(n) = 0$ Clearly all the elements of weight one in $B_2(\phi)$ are covered by the codeword c Also any element $y \in \mathbb{F}_q^n$ of weight two in $B_2(\phi)$ is covered by c if $y(i) \neq 0$ for some i, $1 \leq i \leq R - 1$ The uncovered elements of weight two are all which have both of its nonzero entries $y(i_1)$ and $y(i_2)$ with $R \leq i_1 < i_2 \leq n$ Those elements must be covered by codewords of weight R+1 Let $S = \{s \in C \quad wt(s) = R+1\}$ covers all such remaining elements of weight two in $B_2(\phi)$ We want to calculate the minimum cardinality of S

Consider a $|S| \times n$ matrix $A (= (A_{ij}))$whose row vectors are the elements of S Clearly the number of nonzero entries in A is $|S|(R+1)$ We claim that each column j $R \leq j \leq n$ of A will have at least $\lceil (n-R)(q-1)/R \rceil$ nonzero entries Consider the rows of A say m in number such that for a fixed $j_0$ $R \leq j_0 \leq n$ $A_{ij_0} \neq 0$ W l o g let $j_0 = R$ Consider the $m \times n$ submatrix B of A with all such rows Observe that for all i $1 \leq i \leq m$ $B_{iR} \neq 0$ The number of nonzero entries in the submatrix B is m(R+1) Suppose for some $\ell$ $R+1 \leq \ell \leq n$ the number of nonzero entries in the $\ell$th column of B is (q-2) say

$$B_{i\ell} = b_i, \quad 1 \leq i \leq q-2, \quad b_i \in \mathbb{F}_q \setminus \{0\}$$

Let $B_{iR} = a_i$ $1 \leq i \leq q-2$ $a_i \in \mathbb{F}_q \setminus \{0\}$ Then there exists an element $d \in \mathbb{F}_q^n$ of weight two with its nonzero entries $d(R) \neq a_i$ and $d(\ell) \neq b_i$ $1 \leq i \leq q-2$ which will remain uncovered Hence, every column j $R + 1 \leq j \leq n$ in the submatrix B has at least (q-1) nonzero entries By counting the nonzero entries of B, we have

$$m(R+1) \geq (n-R)(q-1) + m$$

Since m is an integer, we have

$$m \geq \left\lceil \frac{(n-R)(q-1)}{R} \right\rceil$$

Now counting the nonzero entries of **A** we have

$$|S|(R+1) \geq (n-R+1)\lceil (n-R)(q-1)/R \rceil$$

i e

$$|S| \geq \left\lceil \frac{n - R + 1}{R + 1} \left\lceil \frac{(n-R)(q-1)}{R} \right\rceil \right\rceil \quad \blacksquare$$

Lemma 5 4 Let $x \in \mathbb{F}_q^n$ Then for any code with covering radius R and $R < n \leq 2R$ we have

$$\min \left\{ A_{R+1}(x) \quad \lambda_0(x) = \quad = A_{R-2}(x) = A_R(x) \right.$$
$$\left. = A_{R\ ?}(x) = 0 \quad A_{R-1}(x) = 1 \right\} = q - 1$$

Proof W l o g let $x = \phi$ Let $c \in C$ be the codeword of weight (R-1) satisfying $c(R) \quad = c(n) = 0$ Following the argument as in Lemma 5 3 the uncovered element in $B_2(\phi)$ are only those elements of weight two which have both its nonzero entries in the last (n-R+1) coordinate places Let $S = \{s \in C \quad wt(s) = R + 1\}$ covers all such elements We claim that the cardinality of S is at least q-1 Suppose that $|S| = q-2$ Let for all $s_1 \in S$ $s_1(i_1) = a_1$ $s_1(i_2) = b_1$, $R \leq i_1 < i_2 \leq n$ and $a_i b_i \in \mathbb{F}_q$ Then there will be an element $y \in \mathbb{F}_q^n$ such that $y(i_1) = \alpha$ $y(i_2) = \beta$ $\alpha\beta \in \mathbb{F}_q \setminus \{0\}$ where for all i, $1 \leq i \leq q-2$, $\alpha \neq a_i$ and $\beta \neq b_i$ Clearly, the distance of y from S will be at least R + 1 a contradiction Hence $|S| \geq q - 1$ Also the set $S = \{s_i \in C \quad 1 \leq i \leq q - 1 \quad wt(s_i) = R + 1\}$ with $s_i(j) = i$ for $R \leq j \leq n$ covers all the elements in $B_2(\phi)$ left uncovered by c (Note that in case $n < 2R$ some nonzero entries of $s_i$'s will occur in the first R - 1 coordinates ) Thus the result follows $\blacksquare$

Lemma 5 5 Let $x \in A\backslash Z$ $d(x, C) = R-1$ $|B_{R+1}(x) \cap C| = 2$ and let $n \geq 2R+1$ Then

$$\min \lambda_{R,2}(x) \geq \left\lceil \frac{R+1}{R+2}\left\lceil \frac{(n-2R)(q-1)}{R+1} \right\rceil + \frac{(R+1)(q-2)}{R+2} \left\lceil \frac{(n-2R)(q-1) + R(q-2)}{R+1} \right\rceil \right.$$
$$\left. + \frac{(n-2R)(q-1)}{R+2}\left\lceil \frac{(n-R)(q-1)}{R+1} \right\rceil \right\rceil \equiv \delta_o(\text{say}) \qquad (5\ 2)$$

Proof We assume that w l o g $x = \phi$ Let $c_1$ and $c_2$ be the codewords of weight (R-1) and (R+1) respectively and w l o g let $c_1(i) = 0$ $R \leq i \leq n$ Clearly all the elements of weight one in $B_2(\phi)$ are covered by $c_1$ Also any element $y \in \mathbb{F}_q^n$ of weight two having a nonzero entry $y(i)$, $1 \leq i \leq R-1$ is covered by $c_1$ Only the elements $y \in \mathbb{F}_q^n$ having both of its nonzero entries $y(i_1)$ and $y(i_2)$ $R \leq i_1 < i_2 \leq n$ will remain uncovered by $c_1$ We assume that w l o g $c_2(i) = 0$ for all $i$ $1 \leq i \leq R-1$ and $2R+1 \leq i \leq n$ and $c_2(j) = a_j \in \mathbb{F}_q^n \backslash \{0\}$ $R \leq j \leq 2R$ Hence the elements of weight two in $B_2(\phi)$ which remains uncovered by $c_1$ and $c_2$ are the followings

(i) All the elements of weight two with at least one nonzero entry in the last (n-2R) coordinate places and no nonzero entry in first R - 1 coordinate place

(ii) All the elements $y \in \mathbb{F}_q^n$ of weight two with $y(i_1) \in \mathbb{F}_q \backslash \{0, a_{i_1}\}$, $y(i_2) \in \mathbb{F}_q \backslash \{0, a_{i_2}\}$ $R \leq i_1 < i_2 \leq 2R$

We now use a counting argument discussed in [12, Lemma 5] to calculate the minimum number of codewords of weight R+2 required to cover the elements in $B_2(\phi)$ left uncovered by $c_1$ and $c_2$

Let $S = \{s \in C \quad wt(s) = R+2\}$ covers all such elements of weight two We count in two different ways the number of triples $(i, \alpha, s)$, $R \leq i \leq n$ $\alpha \in \mathbb{F}_q \backslash \{0\}$ $s \in S$ and $s(i) = \alpha$ For any fixed $s \in S$ the number of such triples will be at most R+2 (since some words of S may have nonzero entries among

the first R-1 coordinates) Hence the total number of such triples will be at most $|S|^{(R+2)}$ Suppose then that $i$ and $\alpha$ are fixed We consider the following two cases

Case I Let $R \le i \le 2R$ For every pair $(j, \beta)$ $2R+1 \le j \le n$ $\beta \in \mathbb{F}_q \setminus \{0\}$ there is at least one $s \in S$ such that $s(i) = a_i$ (the nonzero $i$th coordinate of $c$) $s(j) = \beta$ and for any $s \in S$ with $s(i) = a_i$ there are at most $R+1$ such pairs $(j, \beta)$ Therefore for fixed $i$ and $\alpha$ (in the present case $\alpha = a_i$) there are at least $\lceil (n-2R)(q-1)/(R+1) \rceil$ such triples Hence the total number of such triples $(i, a_i, s)$ with $s(i) = a_i$ $R \le i \le 2R$ will be

$$(R+1)\lceil (n-2R)(q-1)/(R+1) \rceil \tag{5.3}$$

Now for any pair $(i, \alpha)$ $R \le i \le 2R$ $\alpha \in \mathbb{F}_q \setminus \{0, a_i\}$ there will be

(i) $(n-2R)(q-1)$ pairs $(j, \beta)$ where $2R+1 \le j \le n$ and $\beta \in \mathbb{F}_q \setminus \{0\}$

(ii) $R(q-2)$ pairs $(j, \beta)$ where $\beta \in \mathbb{F}_q \setminus \{0, a_j\}$, $R \le j \le 2R$ $j \ne i$

which will be covered by the elements of S

Hence the total number of such triples $(i, \alpha, s)$ such that $s(i) = \alpha \in \mathbb{F}_q \setminus \{0, a_i\}$ with $R \le i \le 2R$ will be at least

$$(R+1)(q-2)\left\lceil \frac{(n-2R)(q-1) + R(q-2)}{R+1} \right\rceil \tag{5.4}$$

Case II Let $2R+1 \le i \le n$ For fixed pair $(i, \alpha)$ $\alpha \in \mathbb{F}_q \setminus \{0\}$ there will be $(n-R)(q-1)$ pairs $(j, \beta)$, $R \le j \le n$, $j \ne i$, $\beta \in \mathbb{F}_q \setminus \{0\}$ which are covered by elements of S Hence the total number of triples $(i, \alpha, s)$ with $2R+1 \le i \le n$ $s \in S$ and $s(i) = \alpha \in \mathbb{F}_q \setminus \{0\}$ will be

$$(n-2R)(q-1)\lceil (n-R)(q-1)/(R+1) \rceil \tag{5.5}$$

Combining (5.3) (5.4) and (5.5), we have

$$|S|^{(R+2)} \ge (R+1)\left\lceil \frac{(n-2R)(q-1)}{R+1} \right\rceil + (R+1)(q-2)\left\lceil \frac{(n-2R)(q-1) + R(q-2)}{R+1} \right\rceil$$

$$+ (n-2R)(q-1)\left\lceil \frac{(n-R)(q-1)}{R+1} \right\rceil$$

$$|S| \geq \left\lceil \frac{R+1}{R+2}\left\lceil\frac{(n-2R)(q-2)}{R+1}\right\rceil + \frac{(R+1)(q-2)}{R+2}\left\lceil\frac{(n-2R)(q-1)+R(q-2)}{R+1}\right\rceil \right.$$

$$\left. + \frac{(n-2R)(q-1)}{R+2}\left\lceil\frac{(n-R)(q-1)}{R+1}\right\rceil\right\rceil \quad \blacksquare$$

Lemma 5 6 Let $x \in \backslash Z$ $d(x\ C) = R - 1$ and let $|B_{R+1}(x) \cap C| = 2$ If $R+2 \leq n \leq 2R$ then

$$\backslash_{R+2}(x) \geq G(n-R+1\ \ q-2\ \ n-R+1)$$

Proof W l o g let $x = \phi$ Let $c_1$ and $c_2$ be the codewords of weight R-1 and R + 1 respectively and let $c_1$ satisfy $c_1(R) = \quad = c_1(n) = 0$ For $x \in F_q^n$ we use the set $S = \{(i\ \alpha) \in F_q \backslash \{0\}\ \ 1 \leq i \leq n \quad x(i) = \alpha\}$ to represent the element x Hence the elements in $B_2(\phi)$ which remains uncovered by $c_1$ are all 2-subsets $\{(i\ \alpha)\ \ (j\ \beta)\}$ $i \neq j$ of the set $X = \{(i\ \alpha) \quad \alpha \in F_q \backslash \{0\} \quad R \leq i \leq n\}$ W l o g we assume that $c_2(i) \neq 0$ for all i, $R \leq i \leq n$ Let $T = \{(j\ \beta)\ \ R \leq j \leq n \quad c_2(j) = \beta\}$ Clearly the elements in $B_2(\phi)$ which remain uncovered by $c_1$ and $c_2$ are all the 2-subsets $\{(i,\alpha)\ (j,\beta)\}$ $i \neq j$ of the set $Y = Y' \setminus T$ Those elements must be covered by codewords of weight R+2 Let $\mathcal{G} = \{G_R\ G_{R+1} \quad G_n\}$ be a partition of X where each part $G_j$ is the set $\{(j\ \alpha) \quad \alpha \in F_q \backslash \{0\ c_2(j)\}\}$ Clearly $|G_j| = q - 2$ Following the proof as in Lemma 5 2, we have

$$A_{R+2}(x) \geq G(n-R+1\ \ q-2,\ n-R+1) \quad \blacksquare$$

Lemma 5 7 Let C be a code of length n and covering radius R with $n \geq 2R+1$ For any $x \in F_q^n$ let $x \in A \backslash Z$, $d(x,C) = R - 1$ and let $|B_{R+1}(x) \cap C| = 3$ Then $A_{R+2}(x) \geq (q-1)^2$

Proof W l o g let $x = \phi$ Let c be the codeword of weight R - 1 satisfying $c(R) = \quad = c(n) = 0$ Hence, the elements in $B_2(x)$ which

remains uncovered by c are all $y \in \mathbb{F}_q^n$ of weight two which have both its nonzero entries from among the last n - R + 1 coordinates W l o g let a and b be the codewords of weight R + 1 satisfying $a(i) = b(i) = 0$ for all i $1 \le i \le R - 1$ Since $n \ge 2R + 1$ $a(i_1) = 0$ and $b(i_2) = 0$ for some $i_1, i_2 \in \{R, R+1, \ldots, n\}$ If $i_1 \ne i_2$, then all $y \in \mathbb{F}_q^n$ of weight two such that $y(i_1) \ne 0$ and $y(i_2) \ne 0$ remain uncovered by c a and b There are $(q-1)^2$ such elements of weight two and those must be covered by codewords d of weight R + 2 with $d(i_1) = y(i_1)$ and $d(i_2) = y(i_2)$ Hence $A_{R+2} \ge (q-1)^2$ If $i_1 = i_2 = i_0$ then all $y \in \mathbb{F}_q^n$ of weight two with $y(i_0) \ne 0$ and $y(j) \ne 0$ $j \ne i_0$ and $R \le j \le n$ remain uncovered by c a and b Those must be covered by codewords d of weight R+2 with $d(i_0) = y(i_0)$ and $d(j) = y(j)$ and the result follow ■

Lemma 5 8 Let C be a code of length n and covering radius R with $R+2 \le n \le 2R$ For any $x \in \mathbb{F}_q^n$, let $x \in A \setminus Z$ $d(x, C) = R - 1$ and let $|B_{R+1}(x) \cap C| = 3$ Then $A_{R+2}(x) \ge (q-3)^2$

Proof W l o g let $x = \phi$ Let c be the codeword of weight R-1 satisfying $c(R) = \cdots = c(n) = 0$ The elements in $B_2(\phi)$ which remains uncovered are all the elements of weight two which have both its nonzero entry in the last (n-R+1) coordinate places W l o g we assume that $c_1$ and $c_2$ be the codewords of weight R + 1 with $c_1(i) \ne c_2(i) \ne 0$ for $R \le i \le n$ (Note that some nonzero entry of $c_1$ and $c_2$ will be from the first (R-1) coordinate places if $n < 2R$) Hence, the elements in $B_2(\phi)$ which remains uncovered by c, $c_1$ and $c_2$ are all the elements $y \in \mathbb{F}_q^n$ of weight two such that

(i) $y(i) \in \mathbb{F}_q \setminus \{0, c_1(i), c_2(i)\}$,

(ii) $y(j) \in \mathbb{F}_q \setminus \{0, c_1(j), c_2(j)\}$

where $R \le i < j \le n$ Those elements must be covered by codewords d of

weight R + 2 with d(i) = y(i) and d(j) = y(j) Thus the result follows ■

From Lemma 5.3 the following corollary is immediate

Corollary 5.9 For $n \geq 2R + 1$ and $x \in A\backslash Z$ let $d(x, C) = R - 1$ and let $|B_{R+1}(x) \cap C| = 1$ If $3 < i < \alpha_0$ then $A_{R+2}(x) \geq 1$

Lemma 5.4 gives the following corollary

Corollary 5.10 For $R + 2 \leq n \leq 2R$ and $x \in A\backslash Z$ let $d(x, C) = R - 1$ and let $|B_{R+1}(x) \cap C| = 1$ If $3 < i < q - 1$ then $A_{R+2}(x) \geq 1$

Lemma 5.11 For $n = 2R+1$ and $x \in A\backslash Z$ let $d(x,C) = R$ and let $|B_{R+1}(x) \cap C| = i_0 + 1$ where $i_0 = \lceil (n-R)(q-1)/(R+1) \rceil = q - 1$ Then,

$$A_{R+2} \geq \left\lceil \frac{R(q-2)}{R+2} \left\lceil \frac{(n-R)(q-1)}{R+1} \right\rceil + \frac{(n-R)(q-1)}{R+2} \left\lceil \frac{R(q-2)}{R+1} \right\rceil \right\rceil$$

$$= \left\lceil \frac{R(q-2)(q-1)}{R+2} + \frac{(n-R)(q-1)}{R+2} \left\lceil \frac{R(q-2)}{R+1} \right\rceil \right\rceil$$

$$\equiv \gamma_1 \quad \text{(say)}$$

Proof W.l.o.g. let $x = \phi$ Let c be the codeword of weight R satisfying $c(R+1) = \cdots = c(n) = 0$ The elements of weight 1 having the nonzero entry from the last (n-R) coordinate places will remain uncovered by c Those must be covered by codewords of weight R + 1 Since $|B_{R+1}(x) \cap C| = \lceil (n-R)(q-1)/(R+1) \rceil + 1$, i.e. there are $\lceil (n-R)(q-1)/(R+1) \rceil$ codewords of weight R + 1 every such codeword d must satisfy $d(i) = 0$ for $1 \leq i \leq R$ The elements in $B_2(\phi)$ which remains uncovered by such codewords of weight (R+1) and the codeword c, will be all elements of weight 2 having exactly one nonzero entry from the first R coordinate places *distinct from the nonzero entry of* c Those must be covered by codewords of weight R + 2 Following the same counting argument as in the proof of Lemma 5.3, the result can be easily verified ■

Lemma 5 12 For $R \geq 2$, $n = 2R + 1$ and $x \in A\backslash Z$, let $d(x\ C) = R$ and let $|B_{R+1}(x) \cap C| = \iota_0 + 2$ where $\iota_0 = \lceil (n-R)(q-1)/(R+1) \rceil = (q-1)$ Then $A_{R+2} \geq (q-3)(q-1)$

Proof W l o g let $x = \phi$ Let c be the codeword of weight R satisfying $c(R+1) = \quad = c(n) = 0$ Since $|B_{R+1}(x) \cap C| = \iota_0 + 2$ there will be $\iota_0+1$ codewords of weight R + 1 and these codewords must cover all the elements in $B_2(\phi)$ of weight 1 with its nonzero entry from among the last (n-R) coordinate places Let $\mathcal{C} = \{c_1 \quad c_2 \quad \quad c_q\}$ be the collection of such codewords of weight R+1 Since each element of weight 1 with its nonzero entry among the last (n-R) coordinates is covered by at least one codeword of $\mathcal{C}$ and since each coordinate position can have (q-1) distinct nonzero entries at most (R+1) nonzero entries of the elements of the collection $\mathcal{C}$ will be there in the first R coordinates Thus there will be at least one coordinate position J $1 \leq J \leq R$ such that $c_i(J) \neq 0$ say $\beta$ for at most one element $c_1$ of $\mathcal{C}$ Hence the coordinate position J will have at most two nonzero entries say $\alpha$ (= c(J)) and $\beta$ (note that $\alpha$ and $\beta$ may not be distinct) Hence elements $y \in \mathbb{F}_q^n$ of weight 2 such that $y(J) \in \mathbb{F}_q\backslash\{0 \quad \alpha \quad \beta\}$ and $y(k) \in \mathbb{F}_q\backslash\{0\}$ for $k \in \{R+1 \quad ,n\}$ will remain uncovered by the codewords c, $c_1$, $c_q$ Those must be covered by codewords d of weight R + 2 with $d(J) = y(J)$ $d(k) = y(k)$ and hence, there must be at least (q-3)(q-1) such codewords ■

Following the same methodology as discussed by Chen and Honkala [12] we give a better estimate of excess in comparison to Lemma 2 1 5 [12 Lemma 5] for few values of q n and R by using the results proved so far Using the notations as in [12], we denote

$$Y_j = \left\{ z \in A \cap Z \quad \text{the code} - z + \left(B_R(z) \cap C\right) \right.$$

has the property that every two of its words agree in at least $j$ nonzero coordinate places and that there are two words agreeing in precisely $j$ nonzero coordinate places $\Big\}$

Observe that $Y_0, Y_1, \ldots, Y_{R-1}$ form a partition of $A \cap Z$

$$M_{R,1} = 1 + n(q-1) + (R-1)(n-R/2)(q-1)^2$$

$$M_R = 1 + R(q-1)(n-R+1) + \binom{R}{2}(q-1)^2$$

$$M_{R,1} = \binom{R+2}{2} + R(R+1)(q-2)$$

$$t(x) = \begin{cases} \binom{R+2}{2}\left\lceil -x/\binom{R+2}{2}\right\rceil + x & \text{if } x \le 0 \\ x & \text{if } x > 0 \end{cases}$$

$$Z_i = \{x \in \mathbb{F}_q^n \quad |B_R(x) \cap C| = i+1\}$$

$$Y = Z \cap B_{R,1}(C)$$

$$i_0 = \lceil (n-R)(q-1)/(R+1) \rceil \quad \varepsilon_0 = i_0(R+1) - (n-R)(q-1)$$

In [12], Chen and Honkala has proved the following lemma

Lemma 5.13 [12 Lemma 6] If $z \in Y_j \cap Z_i$ then

$$|A \cap B_2(z)| \le V_q(n,2) - \Delta_j$$

where $\Delta_j = \binom{R}{j} + \binom{R-j}{2} + j(R-j)$ and

$$E_C(B_2(x)) \ge i\lambda_j$$

where $\lambda_j = \binom{j}{2}(q-1)^2 + j(n-j)(q-1) + (R-j)^2 + j(q-1) + 1$

We introduce the following notations

$$CH_1(q,n,r,i) = i(R+1) + r(M_{R-1} + iM_{R+1} - V_q(n,2) - i(R+1))$$

$$CH_2(q,n,r,i) = i(R+1) + \varepsilon_0 + r(M_R + (i+i_0)M_{R+1} - V_q(n,2) - i(R+1) - \varepsilon_0)$$

$$A(q\ n\ R) = \begin{cases} \alpha_0, & \text{if } n \geq 2R+1 \quad \text{(Lemma 5 3)} \\ q-1 & \text{if } R+1 \leq n \leq 2R \quad \text{(Lemma 5 4)} \end{cases}$$

If $n \geq 2R+1$ then

$$\delta(q\ n\ R\ \imath) = \begin{cases} \delta_0 & \text{if } \imath = 1 \quad \text{(Lemma 5 5)} \\ (q-1)^2 & \text{if } \imath = 2 \quad \text{(Lemma 5 7)} \\ 1 & \text{if } 2<\imath<A(q\ n\ R) \quad \text{(Corollaries 5 9 and 5 10)} \end{cases}$$

If $R+2 \leq n \leq 2R$ then

$$\delta(q\ n\ R\ \imath) = \begin{cases} G(n-R+1\ \ q-2\ \ n-R+1) & \text{if } \imath = 1 \quad \text{(Lemma 5 6)} \\ (q-3)^2 & \text{if } \imath = 2 \quad \text{(Lemma 5 8)} \end{cases}$$

$$\gamma(q\ n\ R\ \imath) = \begin{cases} \gamma_1 & \text{if } \imath = 0 \text{ and } n = 2R+1 \quad \text{(Lemma 5 11)} \\ (q-3)(q-1) & \text{if } \imath = 1 \text{ and } n = 2R+1 \quad \text{(Lemma 5 12)} \end{cases}$$

$$W_1(q\ n\ R\ \imath) = M_{R-1} + \imath M_{R+1} + \delta(q,n\ R,\imath)\binom{R+2}{2} - V_q(n\ 2)$$

$$W_2(q\ n\ R\ \imath) = M_R + (\imath+1_0)M_{R+1} + \gamma(q\ n\ R\ \imath)\binom{R+2}{2} - V_q(n\ 2)$$

**Lemma 5 14** Assume that $x \in A\backslash Z$

(i) If $d(x\ C) = R - 1$ and $|B_{R+1}(x) \cap C| = 1$ then

$$E_C(B_2(x)) \geq \varepsilon_1 = \binom{R+2}{2}\eta(q\ n,R) - \binom{n-R+1}{2}(q-1)^2 \quad \text{where}$$

(a) If $3 \leq n-R+1 < R+2$ then $\eta(q,n,R) = G(n-R+1\ q-1,n-R+1)$

(b) If $n-R+1 \geq R+2$ then $\eta(q,n,R) = G(R+2,q-1,n-R+1)$

(ii) If $d(x,C) = R - 1$ and $|B_{R+1}(x) \cap C| > 1$ then

$$E_C(B_2(x)) \geq \varepsilon_2 \text{ where } \varepsilon_2 = \min_i \varepsilon_2(i) \text{ and}$$

$$A(q,n,R) = \begin{cases} \alpha_0, & \text{if } n \geq 2R+1 \quad \text{(Lemma 5 3)} \\ q-1, & \text{if } R+1 \leq n \leq 2R \quad \text{(Lemma 5 4)} \end{cases}$$

If $n \geq 2R+1$ then

$$\delta(q\ n\ R\ i) = \begin{cases} \delta_0 & \text{if } i = 1 \quad \text{(Lemma 5 5)} \\ (q-1)^2 & \text{if } i = 2 \quad \text{(Lemma 5 7)} \\ 1 & \text{if } 2<i<A(q\ n\ R) \quad \text{(Corollaries 5 9 and 5 10)} \end{cases}$$

If $R+2 \leq n \leq 2R$ then

$$\delta(q\ n\ R\ i) = \begin{cases} G(n-R+1\ \ q-2\ \ n-R+1) & \text{if } i = 1 \quad \text{(Lemma 5 6)} \\ (q-3)^2 & \text{if } i = 2 \quad \text{(Lemma 5 8)} \end{cases}$$

$$\gamma(q\ n\ R\ i) = \begin{cases} \gamma_1 & \text{if } i = 0 \text{ and } n = 2R+1 \quad \text{(Lemma 5 11)} \\ (q-3)(q-1) & \text{if } i = 1 \text{ and } n = 2R+1 \quad \text{(Lemma 5 12)} \end{cases}$$

$$W_1(q\ n\ R\ i) = M_{R-1} + iM_{R+1} + \delta(q,n\ R\ i)\binom{R+2}{2} - V_q(n\ 2)$$

$$W_2(q\ n\ R\ i) = M_R + (i+1_0)M_{R+1} + \gamma(q\ n\ R\ i)\binom{R+2}{2} - V_q(n\ 2)$$

**Lemma 5 14** Assume that $\mathbf{x} \in A\backslash Z$

(i) If $d(\mathbf{x}\ C) = R - 1$ and $|B_{R+1}(\mathbf{x}) \cap C| = 1$ then

$$E_C(B_2(\mathbf{x})) \geq \varepsilon_1 = \binom{R+2}{2}\eta(q\ n\ R) - \binom{n-R+1}{2}(q-1)^2 \quad \text{where}$$

(a) If $3 \leq n-R+1 < R+2$ then $\eta(q,n\ R) = G(n-R+1\ q-1\ n-R+1)$

(b) If $n-R+1 \geq R+2$ then $\eta(q\ n,R) = G(R+2\ q-1,n-R+1)$

(ii) If $d(\mathbf{x}\ C) = R - 1$ and $|B_{R+1}(\mathbf{x}) \cap C| > 1$ then

$E_C(B_2(\mathbf{x})) \geq \varepsilon_2$ where $\varepsilon_2 = \min_i \varepsilon_2(i)$ and

$$\varepsilon_2(l) = \begin{cases} \max\left\{CH_l(q\ n,R,l),\ W_l(q\ n\ R,l)\right\}, & \text{if } 1 \le l \le 2 \\ CH_l(q\ \ n\ R,l) & \text{otherwise} \end{cases}$$

(iii) If $d(\mathbf{x}\ C) = R$ Then

$$E_C(B_2(x) \ge \varepsilon_3 \quad \text{where } \varepsilon_3 = \min_l \varepsilon_3(l)$$

and

$$\varepsilon_3(l) = \begin{cases} \max\left\{CH_2(q\ n\ R\ l)\ \ W_2(q\ n\ R\ l)\right\} & \text{if } l = 0\ 1 \\ CH_2(q\ \ n\ R\ l) & \text{otherwise} \end{cases}$$

Therefore for any $x \in A\backslash Z$ we have

$$E_C(B_2(x)) \ge \varepsilon = \min\{\varepsilon_1\ \ \varepsilon_2\ \ \varepsilon_3\}$$

**Proof** We assume that w l o g $\mathbf{x} = \phi$ In [12 Lemma 5] it has been shown that for $\mathbf{x}\ \ c \in \mathbb{F}_q^n$ $|B_R(c) \cap B_2(\mathbf{x})| = M_l$ if $d(\mathbf{x}\ c) = l$ $l = R\text{-}1$ R or R+1 and $|B_R(c) \cap B_2(\mathbf{x})| = \binom{R+2}{2}$ if $d(\mathbf{x}\ c) = R+2$

(i) For $x \in A\backslash Z$ and $|B_{R+1}(\mathbf{x}) \cap C| = 1$ we have by (2 8)

$$E_C(B_2(\mathbf{x})) = \sum_{c\in C} |B_R(c) \cap B_2(\mathbf{x})| - V_q(n\ 2)$$

$$= M_{R-1} + \binom{R+2}{2} A_{R+2}(\mathbf{x}) - V_q(n\ 2)$$

$$= \binom{R+2}{2} \eta(q\ n\ R) - \binom{n-R+2}{2}(q-1)^2 \text{ (Lemma 5 1 and Lemma 5 2)}$$

which proves the results

(ii) $$E_C(B_2(\mathbf{x})) = \sum_{c\in C} |B_2(\mathbf{x}) \cap B_R(c)| - V_q(n\ 2)$$

$$= A_{R-1}(\mathbf{x})M_{R-1} + A_R(\mathbf{x})M_R + A_{R+1}(\mathbf{x})M_{R+1} + A_{R+2}(\mathbf{x})M_{R+2} - V_q(n\ 2) \qquad (5\ 6)$$

If $|B_{R+1}(\mathbf{x}) \cap C| = l+1 \ge 2$ then from the hypothesis $A_{R-1}(\mathbf{x}) = 1$ and $A_{R+1}(\mathbf{x}) = 1$

In [12, Lemma 5], Chen and Honkala have shown that

$$E_C(B_2(\mathbf{x})) \ge CH_l(q,n,R\ l) \qquad (5\ 7)$$

Now the result follows from (5 6) and (5 7)

(iii) If $d(\mathbf{x}, C) = R$ then from the hypothesis $A_{R-1}(\mathbf{x}) = 0$ and $A_R(\mathbf{x}) = 1$ In [12 Lemma 5] Chen and Honkala have shown that

$$E_C(B_2(\mathbf{x})) \geq CH_2(q, n, R, 1) \tag{5 8}$$

Now the result follows from (5 6) and (5 8) This concludes the lemma ■

If $\varepsilon = \varepsilon_3$ then we have the following result from [12 Theorem 4] where $\varepsilon$ in [12 Theorem 4] is replaced by $\varepsilon$ calculated from Lemma 5 14

**Theorem 5 15** Assume that $q \geq 3$ and $n > R$ If $\varepsilon = \min\{\varepsilon_1, \varepsilon_2, \varepsilon_3\} = \varepsilon_3$ then

$$K_q(n, R) \geq \frac{(V_q(n, 2) - \mu + \varepsilon)q^n}{(V_q(n, 2) - \mu)V_q(n, R) + \varepsilon V_q(n, R-2)}$$

where $\varepsilon_1$, $\varepsilon_2$, $\varepsilon_3$ and $\varepsilon$ are as in Lemma 5 14 and

$$\mu_0 = \binom{R-2}{2}(q-1)^2 + (R-2)(q-1)(n-R+3) + 2 \qquad \mu_1 = 2R^2 - R + 1 - \varepsilon$$

$$\mu = \begin{cases} \mu_1 & \text{if } R = 1 \\ \min\{\mu_0, \mu_1\} & \text{if } R \geq 2 \end{cases}$$

Let

$$A_1 = \{\mathbf{x} \in \mathbb{F}_q^n : d(\mathbf{x}, C) = R-1\}$$

$$A_2 = \{\mathbf{x} \in \mathbb{F}_q^n : d(\mathbf{x}, C) = R\}$$

Clearly, $A_1$ and $A_2$ is a partition of $A$ We follow the same proof as in [12 Theorem 4] with little modification to give the following result

**Theorem 5 16** Assume that $q \geq 3$ and $n > R$ If $\varepsilon = \min\{\varepsilon_1, \varepsilon_2, \varepsilon_3\} = \min\{\varepsilon_1, \varepsilon_2\}$ then

$$K_q(n, R) \geq \frac{(V_q(n,2) - \mu + \varepsilon_3)q^n}{(V_q(n,2) - \mu)V_q(n, R) + \varepsilon V_q(n, R-2) + (\varepsilon_3 - \varepsilon)V_q(n, R-1)}$$

where $\varepsilon_1$, $\varepsilon_2$, $\varepsilon_3$ and $\varepsilon$ are as in Lemma 5 14 and

$$\mu_0 = \binom{R-2}{2}(q-1)^2 + (R-2)(q-1)(n-R+3) + 2, \qquad \mu_1 = 2R^2 - R + 1 - \varepsilon_3$$

$$\mu = \begin{cases} \mu_1 , & \text{if } R = 1 \\ \min\{\mu_0, \mu_1\}, & \text{if } R \geq 2 \end{cases}$$

**Proof** By Lemma 5.13 and Lemma 5.14

$$\sum E_C(B_2(x))$$

$$= \sum_{x \in A \setminus Z} E_C(B_2(x)) + \sum_{l} \sum_{j=0}^{R-1} \sum_{x \in Y_j \cap Z_l} E_C(B_2(x))$$

$$\geq \varepsilon |A| - \varepsilon_3 \left| \bigcup_{j=0}^{R-1} Y_j \right| + (\varepsilon_3 - \varepsilon)|A_2| + \sum_{j=0}^{R-1} \sum_{l} l\lambda_j |Y_j \cap Z_l|$$

In [12, Theorem 4] Chen and Honkala have shown that

$$\sum_{x \in A} E_C(B_2(x)) = \sum_{x \in A} \sum_{l} l |Z_l \cap B_2(x)| = \sum_{l} l \sum_{x \in Z_l} |A \cap B_2(x)|$$

$$\leq \sum_{l} l \sum_{x \in Y \cap Z_l} (V_q(n,2) - \mu_0)$$

$$+ \sum_{j=0}^{R-1} \sum_{l} l \sum_{x \in Y_j \cap Z_l} (V_q(n,2) - \Delta_j)$$

Combining these we get

$$\varepsilon |A| + (\varepsilon_3 - \varepsilon)|A_2| \leq \sum_{l} l |Y \cap Z_l| (V_q(n,2) - \mu_0)$$

$$+ \sum_{j=0}^{R-1} \sum_{l} l |Y_j \cap Z_l| (V_q(n,2) - \Delta_j - \lambda_j + \varepsilon_3)$$

In [12, Theorem 4] it has been shown that

$$\Delta_j + \lambda_j \geq \Delta_0 + \lambda_0 = 2R^2 - R + 1$$

If $R = 1$, then the set $Y$ is empty Therefore

$$\varepsilon|A| + (\varepsilon_3 - \varepsilon)|A_2| \leq (V_q(n,2) - \mu) \sum_1 1|Y \cap Z_1|$$

$$+ (V_q(n,2) - \mu) \sum_1 1|Y_j \cap Z_1|$$

$$= (V_q(n,2) - \mu) \sum_1 1|Z_1|$$

$$= (V_q(n\ 2) - \mu)(|C|V_q(n,R) - q^n)$$

Since $|A| \geq q^n - |C|V_q(n\ R-2)$ and $|A_2| \geq q^n - |C|V_q(n\ R-1)$ we obtain

$$\varepsilon(q^n - |C|V_q(n\ R-2)) + (\varepsilon_3 - \varepsilon)(q^n - |C|V_q(n,R-1))$$

$$\leq (V_q(n,2) - \mu)(|C|V_q(n\ R) - q^n)$$

which proves the result ■

When applied to particular values of n and R, Theorem 5 15 and Theorem 5 16 give the following improvements in the lower bounds for $K_q(n,R)$ $q \geq 3$

**Corollary 5 17** $K_3(14,4) \geq 255$, $K_4(9,4) \geq 23$ (21),

$K_5(7,3) \geq 32$ (30), $K_5(9,3) \geq 330$ (329),

$K_5(9,4) \geq 54$(53)

The values in the parenthesis are from [14, Table 6 2]

**Note 1** In [14 Table 6 2] the values $K_5(9\ 4)$ and $K_5(7,3)$ are from the sphere covering bound Our results give an improvement to these values

**Note 2** The value $K_3(14,4) \geq 255$ is also obtained by Habsieger, but we have obtained the same bound independently

# CHAPTER VI

# CONCLUSION

In the present dissertation we have improved the lower bounds for binary covering codes using simple observation of Zhang [88] and Honkala s [31] results The improvements are due to the use of covering numbers which have been studied extensively by many researchers

To improve the lower bounds on q-ary covering codes we introduce a combinatorial design (called **Group Covering Design**) in the dissertation This design can be seen as a generalisation of covering designs We have shown that results on covering designs get generalised for group covering designs in many cases This leads to improvements in group covering numbers which results in the improvements of the lower bounds for q-ary covering codes The study on covering numbers for block size greater than or equal to five is still open Any further improvements in the covering numbers for block size greater than or equal to five will give us corresponding improvements in group covering numbers (Corollary 3 2 15)

The idea of the group covering designs may be extended for getting improvements in the lower bounds for multiple/mixed covering codes and we feel that a better counting argument than those used in Chapter V will further improve the lower bounds for q-ary covering codes

# BIBLIOGRAPHY


[1] A M Assaf On the covering of pairs by quadruples" *Discrete Math* 61 (1986) 119-132

[2] A M Assaf An application of modified group divisible designs *J Combin Theory* Ser A 68 (1994) 152-168

[3] A M Assaf W H Mills and R C Mullin 'On tricovers of pairs by quintuples $v \equiv 0 \pmod 4$ *Ars Combin* 33(1992) 31-46

[4] A M Assaf W H Mills and R C Mullin 'On tricovers of pairs by quintuples $v \equiv 1 \pmod 4$ *Ars Combin* 33 (1992) 179-191

[5] A M Assaf and N Shalaby On covering designs with block size 5 and index 4 *Ars Combin* 33 (1992) 227-237

[6] D Avidan Group divisible designs *Master's Thesis*

[7] M R Best A contribution to the nonexistence of perfect codes *Ph D thesis* Univ of Amsterdam The Netherlands, 1982

[8] M R Best Perfect codes hardly exist" *IEEE Trans Inform Theory* 29 (1983) 342-345

[9] M C Bhandari and C Durairajan 'A note on bounds for q-ary covering codes *IEEE Trans Inform Theory* 42 (1996) 1640-1642

[10] A Blokhuis and C W H Lam More coverings by room domains *J Combin Theory* Ser A 36 (1984) 240-244

[11] A E Brouwer A Schrijver and H Hanani "Group divisible designs with block size four' *Discrete Math* 20 (1977) 1-10

[12] W Chen and I S Honkala 'Lower bounds for q-ary covering codes *IEEE Trans Inform Theory* 36 (1990), 664-671

[13] G D Cohen, "Applications of coding theory to communication combinatorial problem' *Discrete Math* Vol 36 No 3 (1990) 664-671

[14] G Cohen I Honkala, S Litsyn, and A Lobstein, *Covering Codes* Elsevier Amsterdam (1997)

[15] G D Cohen M G Karpovsky H F Mattson Jr and J R Schatz 'Covering radius — Survey and recent results" *IEEE Trans Inform Theory* 31 (1985), 328-343

[16] G D Cohen, A C Lobstein and N J A Sloane, 'Further results on the covering radius of codes", *IEEE Trans Inform Theory* 32 (1986) 680-694

[17] T J Dickson, On a covering problem concerning Abelian groups", *J London Math Soc* (2) 3 (1971) 222-232

[18] B Du and L Zhu On the existence of (v,8 1)-BIBD' in W D Wallis et al eds *Combinatorial Designs and Application* (Marcel Dekker New York 1990)

[19] P Erdos and H Hanani On a limit theorem in combinatorial analysis *Publ Math Debrecen* 10 (1963) 10-13

[20] H Fernandes and E Rechtschaffen The football pool problem for 7 and 8 matches' *J Combin Theory* Ser A 35 (1985) 109-114

[21] M K Fort and G A Hedlund "Minimal coverings of pairs by triples *Pacific J Math* 8 (1958), 709-719

[22] R L Graham and N J A Sloane, On the covering radius of codes *IEEE Trans Inform Theory* 31 (1985) 385-401

[23] L Habsieger Lower bounds for q-ary coverings by spheres of radius one *J Combin Theory* Ser A 67 (1994) 199-222

[24] G Haggard On the function N(3 2 λ v)' *Congr Numer* 6 (1972) 243-350

[25] M Hall Jr *Combinatorial Theory* (John Wiley and Sons) 1986

[26] H Hanani 'The existence and construction of balanced incomplete block designs *Ann Math Statist* 32 (1961) 361-386

[27] H Hanani On balanced incomplete block designs with blocks having five elements *J Combin Theory* 12 (1972), 184-201

[28] H Hanani Balanced incomplete block designs and related designs *Discrete Math* 11 (1975) 255-369

[29] H Hanani BIBD's with block size seven", *Discrete Math* 77 (1989) 89-96

[30] I S Honkala, Lower bounds for binary covering codes *IEEE Trans Inform Theory* 34 (1988), 326-329

[31] I S Honkala "Modified bounds for covering codes" *IEEE Trans Inform Theory* 37 (1991), 351-365

[32] J D Horton R C Mullin and R G Stanton Minimal covering of pairs by quadruples", *Congr Numer* 3 (1971) 495-516

[33] X Hou, "New lower bounds for covering codes', *IEEE Trans Inform Theory* 36 (1990) 895-899

[34] X Hou, 'An improved sphere covering bound for the codes with n = 3R + 2' *IEEE Trans Inform Theory* 36 (1990) 1476-1478

[35] S M Johnson "A new lower bound for coverings by rook domains", *Utilitas Mathematica* 1(1972), 121-140

[36] J G Kalbfleisch and R G Stanton "A combinatorial problem in matching' *J London Math Soc* (1) 44 (1969) 60-64

[37] J G Kalbfleisch and P H Weiland "Some new results for the covering problem", in W T Tutte (ed ) "*Recent Progress in Combinatorics*" Academic Press N Y (1969) 37-45

[38] H J L Kamps and J H van Lint "The football pool problem for 5 matches *J Combin Theory* Ser A 3 (1967) 315-325

[39] A Klapper, 'The multicovering radii of codes' *IEEE Trans Inform Theory* 43 (1997) 1372-1377

[40] D J Kleitman and J Spencer, "Families of K-independent sets" *Discrete Math* , 6 (1973), 255-262

[41] H Laakso "Nonexistence of nontrivial perfect codes in the case q = $P_1^a P_2^b P_3^c$ e ≥ 3", Ann Univ Turkee (A1) 177 (1979)

[42] P J M van Laarhoven, E H L Aarts J H van Lint, and L T Wille 'New upper bounds for football pool problem for 6 7 and 8 matches", *J Combin Theory* Ser A 52 (1989) 304-312

[43] E R Lamken, W H Mills R C Mullin and S A Vanstone, "Covering of pairs by quintuples", *J Combin Theory* Ser A 44 (1987) 49-68

[44] D Li and W Chen, "New lower bounds for binary covering codes", *IEEE Trans Inform Theory* 40 (1994), 1122-1129

[45] J H van Lint, "Nonexistence theorems for perfect error-correcting codes", *Computers in Algebra and Number Theory (Symp N Y, 1970)*, SIAM-AMS Proc , Vol IV (G Birkhoff and M Hall, Jr , eds ) 89-95, Providence AMS 1971

[46] J H van Lint, "A survey of perfect codes', *Rocky Mountain J Math* 5 (1975) 199-224

[47] J H van Lint, Recent results on covering problems", in T Mora (ed ), "*Applied Algebra Algebraic Algorithms and Error-Correcting Codes*", LNCS (357), Springer-Verlag, Berlin (1989), 7-21

[48] M Livingston and Q F Stout 'Distribution resources in hypercube computers , in G Fox (ed ), '*Proc of Third Conf on Hypercube Multiprocessors*", Pasadena (1988), 222-231

[49] G O Losey, "Note on a theorem of Zaremba *J Combin Theory* 6 (1969), 208-209

[50] F J MacWilliams and N J A Sloane, "*The Theory of Error-Correcting Codes*", North-Holland, Amsterdam 1977

[51] J G Mauldon Covering theorems for groups", *Quart J Math Oxford* (2) 1 (1950) 284-287

[52] W H Mills On the covering of pairs by quadruples I' *J Combin Theory* Ser A 13 (1972), 55-78

[53] W H Mills On the covering of pairs by quadruple II *J Combin Theory* Ser A 15 (1973) 138-166

[54] W H Mills Covering designs I Coverings by a small number of subsets *Ars Combin* 8 (1979) 199-315

[55] W H Mills A covering of pairs by quintuples', *Ars Combin* 18 (1983) 21-31

[56] W H Mills and R C Mullin Covering pairs by quintuples The case v congruent to 3 (mod 4) *J Combin Theory* Ser A 49 (1988) 308-322

[57] W H Mills and R C M u llin Coverings and packings in *Contemporary Design Theory* A Collection of Surveys Wiley, N Y (1992) 371-399

[58] W H Mills and R C Mullin On λ-covers of pairs by quintuples v odd *J Combin Theory* Ser A 67 (1994) 245-272

[59] R C Mullin On the determination of the covering numbers C(2 5 v) *J Combin Math Combin Comp* 4 (1988), 123-132

[60] R C Mullin 'Finite bases for some PBD-closed sets *Discrete Math* 77 (1989) 217-236

[61] R C Mullin D G Hoffman and C C Lindner "A few more BIBD's with k = 6 and λ = 1 *Ann Discrete Math* 34 (1987) 379-384

[62] R C Mullin and J D Horton 'Bicovers of pairs by quintuples v even *Ars Combin* 26 (1988) 197-228

[63] R C Mullin J D Horton, and W H Mills, On bicovers of pairs by quintuples v odd, v ≠ 3 (mod 10)", *Ars Combin* 31 (1991), 3-19

[64] P R J Ostergård "Construction methods for mixed covering codes in M Gyllenberg and L E Persson (eds ) Proc of 21st Nordic Congress of Mathematicians Marcel Dekker N Y (1993)

[65] P R J Östergård, "Construction methods for covering codes' *Report* 25(1993), *Digital System Laboratory* Helsinki Univ Technology

[66] H F H Reuvers, Some Non-existence Theorems for Perfect Codes Over Arbitrary Alphabets, *Ph D thesis*, Eindhoven University of Technology Eindhoven The Netherlands 1977

[67] E R Rodemich, "Coverings by rook domains', *J Combin Theory* 9 (1970) 117-128

[68] J Schonheim "On coverings', *Pacific J Math* 14 (1964), 1405-1411

[69] N J A Sloane 'Covering arrays and intersecting codes" *J Combin Designs* 1(1993) 51-63

[70] R G Stanton Covering theorem in groups (or How to win at football pools) in W T Tutte (ed ) "*Recent Progress in Combinatorics* Academic Press N Y (1969) 21-36

[71] R G Stanton J D Horton and J G Kalbfleisch 'Covering theorems for vectors with special reference to the case of four and five components *J London Math Soc* 1 (1969) 493-499

[72] R G Stanton and J G Kalbfleisch, 'Covering problems for dichotomized matchings *Aequationes Math* 1 (1968), 94-103

[73] R G Stanton and J G Kalbfleisch "Intersection inequalities for the covering problem' *SIAM J Appl Math* 17 (1969) 1311-1316

[74] R G Stanton J G Kalbfliesch and R C Mullin Covering and packing designs Proc of Second Chapel Hill Conf on Combin Mathematics and its Applications Univ of N Carolina Chapel Hill N C (1970) 428-450

[75] G Tarry Le probleme des 36 officiers" *Compt Rend Assoc Fr Av Sci* 1 (1900) 122-123 2 (1901) 170-203

[76] O Taussky and J Todd Covering theorems for groups *Ann Soc Polon Math* 21 (1948) 303-305

[77] A Tietavainen On the nonexistence of perfect codes over finite fields *SIAM J Appl Math* 24 (1973) 88-96

[78] W D Wallis *Combinatorial Design* Marcel Dekker Inc New York and Basel 1988

[79] E W Weber On the football pool problem for 6 matches A new upper bound *J Combin Theory* Ser A 35 (1983) 109-114

[80] G J M van Wee "Improved sphere bounds on the covering radius of codes *IEEE Trans Inform Theory* 34 (1988) 237-245

[81] G J M van Wee Covering Codes, Perfect Codes and Codes from Algebraic Curves', Ph D thesis Eindhoven University of Technology The Netherlands June 1991

[82] G J M van Wee "Bounds on packings and coverings by spheres in q-ary and mixed Hamming spaces", *J Combin Theory* Ser A 57 (1991) 117-129

[83] L T Wille "The football problem for six matches A new upper bound obtained by simulated annealing" *J Comb Theory* Ser A 45 (1987) 171-177

[84] R M Wilson 'An existence theory for pairwise balance designs I II III', *J Combin Theory* Ser A 13 (1972), 220-245 246-273 18 (1975), 71-79

[85] X Wu 'Optimal binary vector quantization via enumeration of covering codes" *IEEE Trans Inform Theory* 43 (1997), 638-645

[86] S K Zaremba A coveı ıng theorem for Abelian groups *J London Math Soc* 26 (1950) 71-72

[87] S K Zaremba Covering problems concerning Abelian groups *J London Math Soc* 27 (1952) 242-246

[88] Z Zhang Linear inequalities for covering codes Part I — Pair covering inequalities *IEEE Trans Inform Theory* 37 (1991) 573-582

[89] Z Zhang and C Lo Linear inequalities for covering codes Part II — Tı iple covering inequalities , *IEEE Trans Inform Theory* 38 (1992) 1648-1662

[90] L Zhu B Du and J Yın Some new balanced incomplete block designs with k = 6 and λ = 1 *Ars Combın* 24 (1987) 167-174

[91] L Zhu Some recent developments on BIBDs and related designs 189-214 *Dıscrete Math* Vol 123(1993) 189-214